



COMUNE DI CASTENASO
Provincia di Bologna

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

ATTO n. 51 del 25/03/2010

**OGGETTO: DOCUMENTO PROGRAMMATICO SULLA SICUREZZA-
DEC.LGS.196/2003- AGGIORNAMENTO**

Il giorno 25 del mese di Marzo dell'anno 2010 alle ore 14:00 nella Sede Comunale, previa l'osservanza di tutte le formalità prescritte dalla legge e dallo Statuto Comunale, sono stati convocati i componenti della Giunta Comunale.

All'appello risultano presenti:

		Pres
- SERMENGHI STEFANO	Sindaco	S
- BIAGI ANDREA	Vice Sindaco	S
- ZERBINI GABRIELE	Assessore	S
- BIANCOLI ALBERTO	Assessore	S
- TONELLI GIORGIO	Assessore Esterno	S
- GIGLIO CONCETTA	Assessore Esterno	S
- TURRINI ELENA	Assessore Esterno	N
-		
-		
-		
-		
-		
Totale Presenti n. 6		Totale Assenti n. 1

Assiste il Segretario Generale Dott. ANDREA FANTI, che provvede alla redazione del presente verbale.

Il Sindaco STEFANO SERMENGHI assume la presidenza e constatata la legalità dell'adunanza dichiara aperta la presente seduta invitando la Giunta a deliberare sull'oggetto sopra indicato.

Area: SEGRETERIA GENERALE

Oggetto: “DOCUMENTO PROGRAMMATICO SULLA SICUREZZA-DEC.LGS.196/2003-AGGIORNAMENTO”

LA GIUNTA COMUNALE

Premesso che:

- in ottemperanza alle disposizioni di cui all'art.180 del dec.lgs.196/2003 "Codice in materia di protezione dei dati personali" con deliberazione di Giunta n.250 del 13 /12/2005 si è provveduto ad approvare il Documento programmatico sulla sicurezza;
- in ottemperanza delle disposizioni di cui all'art.34 lett. g) del citato dec.lgs.196/2003 con deliberazione di Giunta n.47 del 15/04/2008 è stato approvato l'aggiornamento periodico di tale documento predisposto dalla Ditta Altavia Consulting , con sede in Bologna, Via De'Carracci 5/2, all'uopo incaricata con determinazione del Direttore dell'Associazione Valle dell'Idice n.24 del 13/12/2007;
- in ottemperanza delle disposizioni di cui all'art.34 lett. g) del citato dec.lgs.196/2003 con determinazione del Direttore dell'Associazione Valle dell'Idice n.1 del 25.01.2010 è stata incaricata di provvedere all'aggiornamento periodico di tale documento la Ditta Altavia Consulting , con sede in Bologna, Via De'Carracci 5/2, che, già per il passato si è occupata della materia;

Considerato che dalla data dell'ultimo aggiornamento del DPS sono intervenuti mutamenti organizzativi, logistici ed informatici, per cui si rende necessario procedere all'aggiornamento del documento;

Vista la proposta di aggiornamento del DPS presentata dalla Soc. Altavia Consulting in data 25/03/2010 prot. N. 5365;

Ritenuto di dovere approvare il citato documento redatto ai sensi e per gli effetti dell'art.34-comma 1- lett.g) del dec.lgs.196/2003 e del disciplinare tecnico allegato al medesimo decreto sub.B);

Visti i pareri inseriti nella proposta di delibera ed allegati al presente atto ai sensi dell'art. 49 del D.LGS. n. 267 del 18.08.2000;

Con voti unanimi favorevoli, espressi in forma palese, nei modi e nelle forme di legge;

DELIBERA

- o Di approvare , per le motivazioni di cui alle premesse, il Documento programmatico sulla sicurezza aggiornato alla data odierna (All. “A”) ed il Disciplinare Tecnico (All. “B”);
- o Di disporre che:
 - tutte le struttura dell'Ente si adeguino alle prescrizioni contenute nel DPS;
 - il documento venga aggiornato entro il 31/03/2011;
 - dell'avvenuta approvazione del piano venga fatto riferimento nella relazione di accompagnamento a ciascun bilancio consuntivo.
- o Successivamente, con votazione unanime, si rende il presente atto immediatamente eseguibile ai sensi dell'art. 134 c. 4 D.Lgs. 18.8.2000 n. 267

Il presente verbale viene letto, approvato e sottoscritto

IL SINDACO
Avv. Stefano Sermenghi

IL SEGRETARIO GENERALE
Dott. Andrea Fanti



AltaVia Consulting snc di Giuseppe Mazzoli e C.

Internet Networking | e-Business Consultant | Project Management | Organizzazione



Comune di Castenaso

DPS Piano di sicurezza dell'ente

Marzo 2010

Indice

INDICE	2
I REFERENTI	7
Tavola 1. i referenti del Cliente	7
Tavola 2.: i referenti di AltaVia Consulting	7
LA SICUREZZA: PREMESSA	8
PROTEZIONE CONTRO L'ACCESSO INDEBITO ALLE RISORSE ED APPLICAZIONE DEL D.LGS. N. 196/2003.	11
LO SCHEMA DEL PIANO DI SICUREZZA DI MARZO 2010	12
SECUREANALISYS	14
Il censimento delle banche dati dell'ente	14
Regola 19.1 dell'Allegato B al Codice: elenco dei trattamenti di dati personali, sensibili, giudiziari.	14
Tavola 3. Elenco dei trattamenti: informazioni di base	15
Tavola 4. Elenco dei trattamenti: descrizione degli strumenti utilizzati	30
Tavola 5. Elenco dei trattamenti: cessioni a terzi di dati	40
Il censimento dei beni che rientrano nel piano di sicurezza	51
Tavola 6.riepilogo delle sedi dell'ente	51
Tavola 7. Riepilogo del censimento dei beni informatici che rientrano nel piano di sicurezza dell'ente	52
Analisi organizzativa dell'ente	54
Tavola 8.riepilogo degli incaricati	56
Tavola 9.riepilogo dei profili	62
Rapporti con professionisti ed incaricati non dipendenti dell'ente	63
Distribuzione dei compiti e delle responsabilità (regola 19.2 dell'Allegato B al Codice)	64
Tavola 10.distribuzione dei compiti e delle responsabilità	65
L'accesso alle strutture fisiche dell'ente	69
Tavola 11.: assegnazione delle chiavi di accesso ai locali dell'ente	69
Analisi tecnologica dei dati elettronici	76



segue

Analisi ambientale -----	76
Casi particolari: i posti di lavoro delle sedi non collegate alla LAN comunale -----	77
Analisi del sistema di cablaggio -----	77
Analisi dell'architettura LAN/WAN -----	77
LAN -----	77
WAN -----	78
Analisi delle vulnerabilità interne e dell'accesso ai dati -----	78
Analisi delle applicazioni: regola 19.8 dell'Allegato B al Codice -----	80
Tavola 12.riepilogativa del censimento dei software applicativi informatici che rientrano nel piano di sicurezza dell'ente -----	81
Analisi delle comunicazioni verso Internet -----	84
Analisi dei servizi pubblicati sulla rete Internet -----	84
 Analisi dei dati cartacei-----	86
Analisi ambientale -----	86
Analisi delle vulnerabilità interne e dell'accesso dei dati-----	86
 Le criticità dei beni informatici preposti al trattamento dei dati elettronici-----	87
Il fault tolerance -----	87
Tavola 13.: Tabella riepilogativa dei device presenti nell'ente: censimento dei beni informatici -----	88
Il disaster recovery -----	89
Tavola 14.: Tabella riepilogativa dei fattori di criticità per il servizio di disaster recovery -----	90
 L'analisi dei rischi a cui possono essere soggetti i dati elettronici e i dati cartacei: regola 19.3 dell'Allegato B al Codice-----	93
Analisi dei rischi dei dati elettronici -----	93
Presentazione sintetica dei rischi a cui sono soggetti i dati elettronici trattati dal Comune di Castenaso. -----	94
Tavola 15.: I rischi a cui sono soggetti i dati elettronici trattati dal Comune di Castenaso sono di seguito riepilogati: -----	94
Analisi dei rischi dei dati cartacei -----	96
Presentazione sintetica dei rischi a cui possono essere soggetti i dati cartacei trattati dall'ente -----	96
Tavola 16.: I rischi a cui possono essere soggetti i dati cartacei trattati dall'ente possono essere così riepilogati:--	96
 L'analisi dei sistemi di videosorveglianza-----	98
Tavola 17.: Tabella riepilogativa dei sistemi di videosorveglianza-----	98
Adempimenti ottemperati -----	99
DOVERE DI INFORMAZIONE -----	99
MISURE DI SICUREZZA-----	99
DURATA DELL'EVENTUALE CONSERVAZIONE-----	99



segue

La definizione della politica di sicurezza dell'ente	100
Chi-fa-cosa dentro	100
Tavola 18.: chi-fa-cosa dentro	100
Chi-fa-cosa fuori	106
Tavola 19.: chi-fa-cosa fuori	106
Chi, interno, fa cosa da fuori	108
Tavola 20.: chi, interno, fa-cosa da fuori	108
Chi, esterno, può fare cosa da fuori o, in casi definiti, da dentro	110
Tavola 21.: chi, esterno, può fare-cosa, da fuori o, in casi definiti, da dentro	110
Rapporti con aziende esterne all'organizzazione assimilabili a titolari del trattamento: regola 19.7 dell'Allegato B al Codice	112

SECURELAW----- 113

Securelaw: verifica degli adempimenti formali	113
Dati residenti su elaboratori elettronici	113
Tavola 22.: riepilogo adempimenti formali per dati residenti su elaboratori elettronici	113

Securelaw: verifica degli adempimenti sostanziali	115
Adempimenti sostanziali dati elettronici	116
Tavola 23.: riepilogo adempimenti sostanziali per dati residenti su elaboratori elettronici	116

Securelaw: verifica degli adempimenti formali	117
Dati residenti su archivi cartacei	117
Tavola 24.: riepilogo adempimenti formali per dati residenti su archivi cartacei	117
Adempimenti sostanziali dati cartacei	118
Tavola 25.: riepilogo adempimenti sostanziali per dati residenti su archivi cartacei	118

Securelaw: piano formativo degli incaricati: regola 19.6 dell'Allegato B al Codice	119
Tavola 26.: piano di formazione degli utenti	121

DPS DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI: LE AZIONI 125

Dati residenti su supporto cartaceo	125
Analisi dei rischi	125
Analisi dei rischi e delle azioni intraprese per cautela relativamente al trattamento dei dati cartacei: regola 19.4 dell'Allegato B al Codice	125
Tavola 27.: riepilogo dei rischi e delle azioni legate al trattamento dei dati cartacei	125



segue

Dati residenti su elaboratori elettronici	127
Analisi dei rischi	127
Analisi dei rischi e delle azioni intraprese per cautela: regola 19.4 dell'Allegato B al Codice	127
Tavola 28.: analisi dei rischi e azioni intraprese per i dati residenti su supporto elettronico	127
Le operazioni di salvataggio dei dati: regola 19.5 dell'Allegato B al Codice	130
Tavola 29.: riepilogo delle operazioni di salvataggio dei dati	130
I controlli anti-intrusione dall'esterno	131
Tavola 30.: riepilogo delle operazioni di controlli anti-intrusione dall'esterno	131
 AZIONI INTRAPRESE PER IL FAULT TOLERANCE: REGOLA 19.5 DELL'ALLEGATO B AL CODICE	 132
Server Windows NT/200X	132
Server Virtuali	133
Server Linux	133
Server ESXi	134
Switch	134
Firewall e Router	134
 PROCEDURE DA SEGUIRE IN CASO DI FAULT	 136
Server	136
Server Windows 200X	136
Server Linux	137
Server Windows 200X – SQL Server	137
Switch	138
Connessione ad Internet	138
Router e connessioni WAN	138
Linee di collegamento in fibra ottica	139



segue

AZIONI DA INTRAPRENDERE PER IL DISASTER RECOVERY	140
PROCEDURE DA SEGUIRE PER AFFRONTARE UNA SITUAZIONE DI DISASTER RECOVERY	142
Server	142
Procedure da eseguire per i server di cui è presente il servizio di disaster recovery sul software di back-up dei dati	142
Tavola 31.: riepilogo procedure di disaster recovery per la sede del Municipio di Castenaso legate ai dati	142
Router e Wan Link	144
Tavola 32.: riepilogo procedure di disaster recovery per la sede di Castenaso legate ai Wan Link	144
DOCUMENTI AGGIUNTIVI: DISCIPLINARE INTERNET	145
AMMINISTRATORI DI SISTEMA	146
RELAZIONE ALLEGATA AL BILANCIO	147
CONCLUSIONI	148
TERMINI E DEFINIZIONI	149

I referenti

Riepiloghiamo ora i referenti del Cliente e di AltaVia Consulting Snc di Giuseppe Mazzoli e C. coinvolti nel progetto.

Tavola 1. i referenti del Cliente

Nome e Cognome	Mansione	Funzione specifica nel progetto
Francesco Capasso	Istruttore informatico	Fornitore di informazioni

Tavola 2.: i referenti di AltaVia Consulting

Nome e Cognome	Mansione	Funzione specifica nel progetto
Giuseppe Mazzoli	Progettista	Coordinatore

La sicurezza: premessa

Con l'entrata in vigore del “*Codice in materia di protezione dei dati personali*” il legislatore sancisce che il diritto alla riservatezza, all'identità personale e alla protezione dei dati riferiti a persone fisiche o giuridiche sono da annoverarsi tra i diritti fondamentali. Di conseguenza qualsiasi *trattamento* di dati personali deve svolgersi nel rispetto della dignità del soggetto interessato sottoposto al trattamento.

Da quanto esposto sopra deriva la necessità di rafforzare, in un quadro di evoluzione tecnologica, le misure di sicurezza contro i rischi di distruzione o perdita, anche accidentale, dei dati personali, di accesso non autorizzato o di uso improprio dei dati stessi. A tal fine alle precauzioni già previste nella normativa precedente (password, codici identificativi, antivirus etc.), se ne aggiungono altre come: password di non meno di otto caratteri, autenticazione informatica, sistemi di cifratura, procedure per il ripristino dei dati, ecc., nonché la tenuta di un aggiornato documento programmatico sulla sicurezza.

Nonostante sia utopistico credere che possa esistere la sicurezza assoluta, questo non esime qualsiasi titolare, responsabile o incaricato del trattamento dei dati personali a predisporre un piano di sicurezza dell'ente. Occorre però individuare, in via preliminare, quali sono i requisiti minimi di sicurezza di un sistema informativo basato su strumenti elettronici o su strumenti cartacei per poterli applicare al sistema stesso nella totalità o in parte.

L'obiettivo è quindi quello di stabilire il livello di sicurezza da raggiungere in relazione al valore del bene intangibile da proteggere (informazione) ed al rischio sostenibile, senza ridurre la possibilità di fruizione dello stesso.

Un sistema informativo deve, quindi, avere un sistema di protezione contro i seguenti rischi:

- accesso indebito alle risorse;
- azioni dolose;
- errori operativi;
- manomissioni o furti;
- fault di servizi;
- eventi dannosi o disastrosi

offrendo al contempo garanzia di:

- autenticità e integrità delle registrazioni elettroniche

ed assicurando:

- facilità di auditing

Per **accesso indebito alle risorse** s'intende che dati, programmi e strumenti di comunicazione devono essere protetti da accessi non autorizzati, in ottemperanza al d.lgs. n. 196/2003.

Per **protezione da azioni dolose** s'intende che devono esistere procedure e strumenti per proteggere le risorse del S.I.



segue

da azioni particolari come modifica o copia di informazioni, messaggi, file, programmi da parte di persone non autorizzate, uso non autorizzato dei privilegi di sistema, dirottamento o duplicazione di informazioni o programmi da parte di persone non autorizzate, bombe logiche, cavalli di Troia, virus.

Per **protezione dagli errori operativi** s'intende che il S.I. deve essere progettato in modo che errori operativi non arrechino danni alle risorse hardware e software, che le operazioni critiche siano attivabili solo da personale autorizzato e che devono essere previsti strumenti per ripristinare lo stato corretto del sistema nel caso vengano rilevati errori operativi.

Per **protezione da manomissioni o furti** s'intende che i server dell'ente, nonché i documenti cartacei, devono essere custoditi in locali protetti in cui l'accesso è permesso solo agli incaricati per lo svolgimento di compiti ad essi assegnati.

Per **protezione contro il fault o la caduta di alcuni servizi**, s'intende che è opportuno che esista una procedura in grado di far ripartire un servizio più o meno critico, più o meno importante, servizio caduto in seguito ad un guasto hardware e/o software, con i tempi ed i modi definiti dal "manuale della sicurezza".

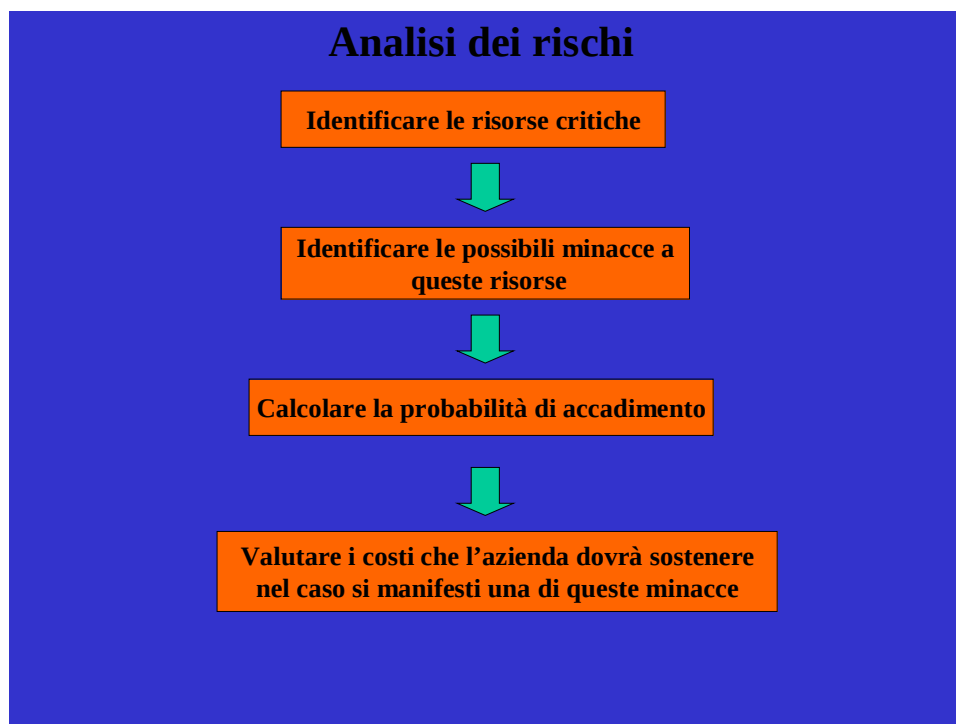
Infine per **protezione contro eventi dannosi o disastrosi** s'intende che è necessario che il sistema informativo preveda contromisure per tutelarlo da eventi dannosi (assenza di alimentazione elettrica o condizionamento) o disastrosi (incendi ecc.).

La **garanzia** che deve essere offerta dal sistema informativo è relativa all'**autenticità dei dati**, ovvero deve essere disponibile un meccanismo per associare ad una unità di registrazione l'identificativo dell'utente che l'ha generata nella forma in cui essa è memorizzata, con una prova incontestabile, e all'**integrità del dato stesso**. Per integrità dei dati gestiti e registrati a livello applicativo; si afferma che il compito del S.I. è quello di garantire l'integrità logica (*coerenza e consistenza*) e fisica (*esistenza di copie o di salvataggi*) di tali dati.

Per quanto riguarda i **requisiti di auditing** essi riguardano quelle caratteristiche del sistema informativo che possono facilitare le attività ispettive necessarie per assicurare il mantenimento del livello di sicurezza.

Il primo passo da fare per decidere la politica da seguire nel garantire la sicurezza di un sistema è l'analisi del rischio. L'obiettivo di tale analisi è quello di identificare le minacce alle risorse critiche del sistema per valutare le perdite derivanti dal verificarsi di tali minacce e potere eventualmente giustificare i costi da sostenere per la gestione della sicurezza.

Il processo è quindi il seguente:



L'analisi dei rischi, oggetto del presente lavoro, non tratta in dettaglio le probabilità di accadimento dei rischi stessi, né i costi, legati al mancato uso dei sistemi, in quanto si da per scontato che tali eventi si verifichino e che i costi ad essi associati siano ingenti.

Protezione contro l'accesso indebito alle risorse ed applicazione del d.lgs. n. 196/2003.

In primo luogo è utile riassumere quali sono gli strumenti ordinari di sicurezza che gli utenti già utilizzano per accedere ai dati elettronici e/o ai dati cartacei.

Ogni utente è dotato di uno username ed una password per l'accesso alla rete dell'ente. Detto username è fisso ed è assegnato dal gruppo sistemistico del servizio sistemi informativi del Comune di Castenaso.. La password invece è gestita dall'utente che deve forzatamente modificarla ogni 90 giorni. Il primo identificativo dell'utente permette l'accesso a tutte le risorse di rete; alcuni servizi però richiedono, per problemi tecnici legati all'integrazione degli utenti nel Dominio Microsoft (il sistema di directory dell'ente), un ulteriore livello di identificazione quale, per esempio, l'accesso alla posta elettronica.

Ciascun application server ha poi la sua applicazione: Contabilità, Gestione del Personale, Lotus Domino Notes ecc. Gli utenti hanno, a questo punto, un ulteriore livello di autenticazione sulla procedura: uno username ed una password fissi sono assegnati all'utente a questo livello per ciascuna delle applicazioni software alle quali ha accesso.

Per ciò che concerne le misure minime di sicurezza richieste dalla nuova normativa, l'ente si è opportunamente attrezzato in base a quanto previsto dal Titolo V, Capo II del Codice in materia di protezione dei dati personali e dall'Allegato B dello stesso Codice.

In primo luogo occorre precisare che il Comune di Castenaso tratta dati che si configurano sia come dati personali, sia come dati sensibili, e ancora dati giudiziari in base all'interpretazione letterale del d.lgs. n. 196/2003. In secondo luogo durante le sessioni formative ai dipendenti è presentato il regolamento al quale attenersi nel trattamento dei dati nello svolgimento dei compiti assegnati. Sono stati, inoltre, definiti il responsabile del trattamento dei dati, gli incaricati autorizzati a compiere specifiche operazioni e le procedure relative alla gestione dei dati stessi.

Tutti i dettagli del piano di sicurezza verranno approfonditi nei capitoli successivi.

Lo schema del piano di sicurezza di marzo 2010

Il piano di sicurezza 2010, è in continuità con quello 2008, che aveva completamente rivisto rispetto agli anni precedenti l'impostazione, in quanto si vuole mettere in risalto le misure adottate dall'ente, che superano di gran lunga quelle minime previste dalla nuova normativa in materia di sicurezza dell'ente dei dati.

L'intero lavoro è denominato DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI ai sensi del d.lgs. n. 196/2003, ma si presenta come un vero e proprio PIANO DI SICUREZZA DELL'ENTE.

Il PIANO DI SICUREZZA DELL'ENTE prevede due ambiti di analisi:

- un'analisi interna articolata in otto punti denominata *secureanalysis*;
- un'analisi legislativa per accertare il rispetto dei requisiti richiesti dalla normativa attualmente in vigore denominata *securelaw*.

Prosegue poi con il Documento programmatico sulla sicurezza vero e proprio

Secureanalysis

Gli obiettivi di questa fase, come sopra anticipato, sono nove:

1. censimento delle banche dati trattati;
2. definizione e censimento di tutti i beni che rientrano nel piano di sicurezza dell'ente;
3. analisi organizzativa dell'ente;
4. analisi tecnologica dei dati elettronici:
 - a. analisi ambientale;
 - b. analisi del sistema di cablaggio;
 - c. analisi dell'architettura LAN e WAN;
 - d. analisi delle vulnerabilità interne e dell'accesso ai dati;
 - e. analisi delle comunicazioni verso Internet;
 - f. analisi dei servizi pubblicati sulla rete Internet.
5. analisi tecnologica dei dati cartacei:
 - a. analisi ambientale;
 - b. analisi delle vulnerabilità interne e dell'accesso ai dati.
6. Definizione dei livelli di criticità dei beni informatici preposti al trattamento dei dati elettronici



segue

7. l'analisi dei rischi a cui possono essere soggetti i dati elettronici e i dati cartacei;
8. analisi dei sistemi di videosorveglianza;
9. Definizione di una politica di sicurezza dell'ente.

Securelaw

Con la fase "securelaw" si intende verificare che tutti i requisiti normativi circa il rispetto del d.lgs. n. 196/2003 denominato "Codice in materia di protezione dei dati personali" siano rispettati ed assecon dati.

Per fare ciò è necessario affrontare i seguenti quattro punti:

1. verifica degli adempimenti formali;
2. verifica degli adempimenti sostanziali;
3. piano formativo degli incaricati;
4. predisposizione di un *Documento programmatico sulla sicurezza dei dati*.

Si incomincia ora con l'analisi dei singoli punti della *secureanalysis*.



Secureanalysis

Il censimento delle banche dati dell'ente

In questa sezione del documento censiamo tutti le banche dati, personali e sensibili che sono oggetto di trattamento all'interno dell'ente.

Regola 19.1 dell'Allegato B al Codice: elenco dei trattamenti di dati personali, sensibili, giudiziari.



segue

Tavola 3. Elenco dei trattamenti: informazioni di base

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
1.	Gestione protocollo comunale.	X		AREA AFFARI GENERALI SERVIZIO URP segreteria affari generali		Cartacei-elettronici
2.	Sito Internet, customer satisfaction (attività in fase di preparazione).			AREA AFFARI GENERALI SERVIZIO URP		Cartacei-elettronici
3.	Contrassegni invalidi, denunce infortuni, denunce cessione alloggi, licenze caccia/pesca, ritiro richieste iscrizione servizi comunali.	X		AREA AFFARI GENERALI SERVIZIO URP		Cartacei-elettronici
4.	Gestione reclami.			AREA AFFARI GENERALI SERVIZIO URP		Cartacei-elettronici
5.	Raccolta originali atti (delibere, determine, ordinanze), convocazioni giunta e consiglio.	X		AREA AFFARI GENERALI SERVIZIO URP - Segreteria Affari generali/istituzionali		Cartacei-elettronici
6.	Notifiche, albi, difensore civico, mediatore sociale.	X	X	AREA AFFARI GENERALI SERVIZIO URP - Segreteria		Cartacei-elettronici
7.	Gestione anagrafe-stato civile -leva –elettorale.	X		AREA AFFARI GENERALI Servizi demografici		Cartacei-elettronici
8.	Tenuta registri.	X		AREA AFFARI GENERALI Servizi demografici		Cartacei-elettronici
9.	Rilascio certificati.	X		AREA AFFARI GENERALI Servizi demografici		Cartacei-elettronici
10.	Documentazione amministrativa (autentiche, copie conformi).	X		AREA AFFARI GENERALI Servizi demografici		Cartacei-elettronici
11.	Statistiche.	X		AREA AFFARI GENERALI Servizi demografici		Cartacei-elettronici
12.	Procedimenti elettorali.	X		AREA AFFARI GENERALI Servizi demografici		Cartacei-elettronici
13.	Tenuta albi (Presidenti, scrutatori, Giudici popolari).	X		AREA AFFARI GENERALI Servizi demografici		Cartacei-elettronici
14.	Gestione dati trasmessi da pompe funebri in relazione al rilascio autorizzazione trasporto salme e trasporto e cremazione.	X		AREA AFFARI GENERALI Servizi demografici		Cartacei-elettronici

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
15.	Gestione dati trasmessi da pompe funebri in relazione al rilascio autorizzazione trasporto salme e trasporto e cremazione.			AREA AFFARI GENERALI Servizi demografici		Cartacei-elettronici
16.	Abbonamenti agevolati per mezzi pubblici: assistenza ai richiedenti per compilazione modulo per concessione abbonamento agevolato.			AREA AFFARI GENERALI Servizio URP		Cartacei, elettronici
17.	Gestione dati di tutti i beneficiari per anno solare al fine della compilazione dell'Albo dei beneficiari di provvidenze economiche (DPR 7.4.2000 n. 118).			AREA AFFARI GENERALI Servizio Segreteria/Affari Generali		Cartacei-elettronici
18.	Raccolta dati richiedenti al momento della domanda di iscrizione al servizio.			AREA AFFARI GENERALI – Servizio URP		Cartacei Elettronici
19.	Elaborazione atti di difesa/costituzione in giudizio dell'ente.			AREA AFFARI GENERALI – Legale/Gare e Contratti		Cartacei Elettronici
20.	Gestione contenzioso stragiudiziale (accordi di transazione e comunicazioni).			AREA AFFARI GENERALI – Legale/Gare e Contratti		Cartacei Elettronici
21.	Elaborazione contratti/disciplinari di incarico. Trasmissione dati collaboratori esterni (incarichi professionali)			AREA AFFARI GENERALI – Legale/Gare e Contratti	Ministero Funzione Pubblica/Anagrafe delle Prestazioni	Cartacei Elettronici
22.	Trasmissione dati anagrafici ditte aggiudicatarie di lavori pubblici, servizi e forniture.			AREA AFFARI GENERALI – Legale/Gare e Contratti	Ufficio Territoriale del Governo - Bologna	Cartacei Elettronici
23.	Richiesta certificazioni (casellario e carichi pendenti) di ditte aggiudicatarie di lavori pubblici, servizi e forniture.			AREA AFFARI GENERALI – Legale/Gare e Contratti	Procura della Repubblica c/o Tribunale di Bologna	Cartacei Elettronici
24.	Gestione dati anagrafici di studi legali.			AREA AFFARI GENERALI – Legale/Gare e Contratti		Cartacei Elettronici
25.	Dati anagrafici per richiesta dei Durc delle ditte aggiudicatarie di lavori pubblici, servizi e forniture ai soli fini della stipulazione del contratto d'appalto			AREA AFFARI GENERALI – Legale/Gare e Contratti	Sportello Unico (Inps, Inail, Ceda, CME) Tutte le u.o. operative che affidano appalti, coinvolte in sede di liquidazione dei compensi agli appaltatori	Cartacei Elettronici

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
26.	Calcolo relativo alla minore contribuzione di ogni utente del servizio nido in base alla propria quota agevolata rispetto alla retta massima, al fine della compilazione dell'Albo dei beneficiari di provvidenze economiche (DPR 7.4.2000 n. 118).			AREA AFFARI GENERALI Servizio Servizi educativi e scolastici	Ditta esterna, Banca Dati INPS, Azienda Usl Bologna, Provincia di Bologna, Regione Emilia Romagna	Cartacei-elettronici
27.	Gestione dati di tutti i beneficiari per anno solare al fine della compilazione dell'Albo dei beneficiari di provvidenze economiche (DPR 7.4.2000 n. 118).			AREA AFFARI GENERALI Servizio Segreteria/Affari Generali		Cartacei-elettronici
28.	Gestione dati di tutti i beneficiari per anno solare per rendicontazione contributi straordinari (art. 158 Dlgs. 267/2000) e per compilazione dell'Albo dei beneficiari di provvidenze economiche (DPR 7.4.2000 n. 118).			AREA AFFARI GENERALI Servizio Segreteria/Affari Generali		Cartacei-elettronici
29.	Periodico comunale, comunicati stampa, mailing list ,			AREA AFFARI GENERALI Servizio URP	Direttore del periodico comunale	Cartacei-elettronici
30.	Gestione anagrafica contribuenti Imposta comunale sugli immobili, Tassa Rifiuti Solidi Urbani, Tassa Occupazione Spazi ed Aree Pubbliche.			AREA CONTROLLO DI GESTIONE E TRIBUTI U.O. Tributi – Riscossione coattiva entrate comunali	Consorzio Nazionale Concessionari di Bologna	Cartacei-elettronici
31.	Gestione dati relativi alla situazione reddituale di contribuenti che fanno richiesta di particolari agevolazioni in materia di tributi locali quali I.C.I. e T.A.R.S.U.			AREA CONTROLLO DI GESTIONE E TRIBUTI U.O. Tributi – Riscossione coattiva entrate comunali	Consorzio Nazionale Concessionari di Bologna	Cartacei-elettronici
32.	Gestione dati relativi alla situazione sanitaria (presenza all'interno del nucleo familiare di portatori di handicap) di contribuenti che fanno richiesta di particolari agevolazioni in materia di I.C.I.			AREA CONTROLLO DI GESTIONE E TRIBUTI U.O. Tributi – Riscossione coattiva entrate comunali	Consorzio Nazionale Concessionari di Bologna	Cartacei-elettronici
33.	Gestione anagrafica concessionari posizioni cimiteriali e defunti.			AREA CONTROLLO DI GESTIONE E TRIBUTI U.O. Tributi – Riscossione coattiva entrate comunali		Cartacei-elettronici
34.	Gestione dati relativi a Fornitori/Prestatori di servizi/incaricati/Personale Dipendente del Comune di Castenaso (anagrafica persone fisiche/giuridiche; coordinate bancarie; gestione fatture).	X		AREA BILANCIO Servizio Ragioneria e Bilancio	Studio esterno (consulente in materia fiscale).	Cartacei-elettronici

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
35.	Tenuta presso l'Ufficio ragioneria di atti (determinazioni/delibere) rilevanti ai fini contabili predisposti da altri servizi/settori e contenenti anagrafiche di soggetti percettori di contributi, ricoveri in istituti convenzionali ecc.	X		AREA BILANCIO Servizio Ragioneria e Bilancio	Studio esterno (consulente in materia fiscale).	Cartacei-elettronici
36.	Gestione di dati relativi ad alcuni fornitori (ragione sociale, indirizzo, n° di telefono e fax, coordinate bancarie, ecc. dei fornitori del Servizio Economato).			AREA BILANCIO Servizio Provveditorato Economato	Ditta Esterna (ADS S.P.A.)	Cartacei-elettronici
37.	Gestione dati relativi ai sinistri avvenuti nel territorio del Comune e inerenti le Polizze Assicurative Comunali (ad es. RCT/O, RC Auto, Infortuni Alunni,...).			AREA BILANCIO Servizio Provveditorato Economato	ASSITECA BSA VIA GIARDINI 474/M MODENA fino al 31.03.2010. MARSH dal 01.04.2010 per un triennio	Cartacei-elettronici
38.	Gestione di dati relativi ai dipendenti aventi diritto al vestiario, come – ad esempio – certificati medici che implicano l'esonero dall'utilizzo di calzature antinfortunistiche.			AREA BILANCIO Servizio Provveditorato Economato		Cartacei-elettronici
39.	Gestione dati relativi agli oggetti smarriti (il Servizio Economato riceve e custodisce i verbali di rinvenimento redatti dalla Polizia Municipale e redige i verbali di riconsegna al proprietario o al ritrovatore).			AREA BILANCIO Servizio Provveditorato Economato		Cartacei-elettronici
40.	Aggiornamento anagrafica fornitori/clienti	X		AREA BILANCIO Servizio Ragioneria e Bilancio	Ditta esterna (aggiornamento archivi)	Cartacei-elettronici
41.	Osservatorio provinciale per la registrazione degli accessi sia diretti sia telefonici allo Sportello Sociale	X		AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Sociali,	Ditta esterna (Softech di Bologna) Provincia	Elettronici
42.	Servizio Assistenza Domiciliare (SAD): gestione anagrafica utenti per accesso al servizio (tramite programma informatico GARSIA); gestione cartelle individuali per utente (contengono anche dati sensibili).	X		AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Sociali, Politiche Abitative, Sanità	Ditta esterna (Softech di Bologna)	Cartacei-elettronici
43.	Orti: gestione anagrafica per assegnazione e relativa bollettazione retta annuale (tramite programma SOSIA).			AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Sociali, Politiche Abitative, Sanità	Ditta esterna (Softech di Bologna) URP (raccolta domande)	Cartacei-elettronici
44.	Abbonamenti agevolati per mezzi pubblici: assistenza ai richiedenti per compilazione modulo per concessione abbonamento agevolato sia per studenti che anziani e disabili	X		AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Sociali, Politiche Abitative, Sanità, Servizi educativi	URP (raccolta domande)	Cartacei, elettronici

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
45.	Politiche abitative: gestione anagrafica richiedenti ed assegnatari alloggi ERP, appartamenti Servizio Pronto Emergenza abitativa ed alloggi a canoni agevolati; gestione abitativa (contratto, importo affitto, eventuale provvedimento sfratto, dimensioni e caratteristiche di idoneità dell'alloggio), bollettazione utenti Pronto Emergenza Abitativa; predisposizione graduatorie pubbliche per richiedenti alloggi ERP o a canone agevolato.	X		AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Sociali, Politiche Abitative, Sanità	ACER (Azienda Casa Emilia Romagna)	Cartacei, elettronici
46.	Raccolta domande e relativa istruttoria ai fini della concessione del contributo per l'affitto (ai sensi della L. 431/98, della L.R. n. 24/2001)	X		AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Sociali, Politiche Abitative, Sanità	Regione Emilia Romagna	Cartacei, elettronici
47.	Centro Accoglienza Extracomunitari: gestione anagrafica (oltre ai dati anagrafici, nazionalità, permesso/carta di soggiorno valida), condizioni sociali e sanitarie, lavorative e abitative dei richiedenti per assegnazione posto letto; gestione utenti per bollettazione rette mensili (tramite programma SOSIA).	X		AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Sociali, Politiche Abitative, Sanità	Ditta esterna (Softtech di Bologna),	Cartacei, elettronici
48.	Contributi/benefici economici: gestione richiedenti/utenti (persone fisiche e associazioni) contributi comunali (unatum, esenzioni ticket, contributi per handicap, contributi per integrazione rette di ricovero in struttura);riduzioni /esenzioni rette scolastiche e per l'Asilo Nido; gestione richiedenti assegno per nucleo numeroso e per maternità (Legge 448/98 artt.65-66); gestione utenti per contributo regionale a sostegno dell'affitto, il relativo contributo viene calcolato tramite programma informatico regionale.	X		AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Sociali, Politiche Abitative, Sanità	Banca Dati INPS, Regione Emilia Romagna	Cartacei-elettronici
49.	Invalidità civili : gestione pratiche utenti per concessione provvidenze economiche; gestione dichiarazioni di responsabilità che i titolari di accompagnamento sono tenuti a fare annualmente.	X		AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Sociali, Politiche Abitative, Sanità	Comune di Bologna	Cartacei-elettronici

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
50.	Interventi in favore di anziani non-autosufficienti (L.R. 5/94): gestione utenti per accesso alla rete dei servizi socio-sanitari integrati (tramite programma informatico GARSIA).	X		AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Sociali, Politiche Abitative, Sanità	Ditta esterna (Softech di Bologna), ASL BOLOGNA Distretto Pianura Est	Cartacei-elettronici
51.	Certificazioni ISEE: attestazione condizioni economiche ai fini della concessione di contributi ed agevolazioni tariffarie di vario tipo nonché per l'ammissione ai vari servizi che lo prevedono fra i requisiti di accesso (calcolata ai sensi D.Lgs n. 109/98 e successive modificazioni ed integrazioni), tramite programma INPS.	X		AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Sociali, Politiche Abitative, Sanità, Servizi educativi	Banca Dati INPS	Cartacei-elettronici
52.	Raccolta dati dei nuclei familiari richiedenti il servizio, attraverso il modulo di domanda e dichiarazione sostitutiva unica finalizzata al calcolo dell'indicatore ISEE (facoltativa), al fine della formazione delle graduatorie di ammissione (Regolamento comunale servizi educativi per la prima infanzia delib. C.C. n. 6 del 4.02.2009) e della successiva comunicazione agli interessati dell'ammissione/non ammissione al nido.	X		AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Educativi e Scolastici, Sport – Servizio Nido	Ditta esterna (Softech di Bologna), Banca Dati INPS, Azienda Usl Bologna, URP (raccolta domande)	Cartacei-elettronici
53.	Gestione anagrafica iscritti, al fine della bollettazione del servizio.			AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Educativi e Scolastici, Sport – Servizio Nido	Ditta esterna, Banca Dati INPS	Cartacei-elettronici
54.	Raccolta schede di anamnesi per i nuovi ammessi ed inoltro delle stesse alla ASL, al fine dello svolgimento degli opportuni controlli sanitari da parte della stessa.			AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Educativi e Scolastici, Sport – Servizio Nido	Azienda Usl Bologna	Cartacei-elettronici
55.	Gestione anagrafica richiedenti ed iscritti			AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Educativi	Ufficio Relazioni con il Pubblico	Cartacei-elettronici
56.	Raccolta dati richiedenti al momento della domanda di iscrizione al servizio.			AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Educativi e Scolastici, Sport – Centri Estivi	Ditta esterna che gestisce in appalto tali servizi comunali	Cartacei-elettronici

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
57.	Gestione anagrafica richiedenti ed iscritti. – Gestione dati utenti Sportello d'ascolto 0-6 anni (intervento di sostegno alla genitorialità)	X		AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Educativi	Ufficio Relazioni con il Pubblico (Raccolta domande). Coordinatrice pedagogica incaricata Dott.ssa Licia Vasta	Cartacei
58.	Gestione anagrafica iscritti per organizzazione del servizio (comunicazione degli stessi al gestore in appalto del servizio).		X	ISTITUZIONE SISTER (Refezione, Trasporto scol., parascolastici, centri estivi)	Ditta esterna che gestisce in appalto tali servizi comunali (Società Dolce di Bologna)	Cartacei
59.	Gestione anagrafica iscritti al fine della bollettazione del servizio (Indirizzi e criteri per l'applicazione delle rette relative ai servizi educativi e scolastici delib. C.C. n. 7 del 4.02.09).			ISTITUZIONE SISTER	Ditta esterna che gestisce in appalto tali servizi comunali (Ditta Softech di Bologna)	Elettronici
60.	Raccolta dati richiedenti al momento della domanda di iscrizione al servizio.			AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Educativi e Scolastici, Sport – Servizi Scolastici (refezione, pre/post scuola, custodia, trasporto) Tramite URP	Ditta esterna che fornisce i software SOSIA, Gradus, Sportello (Ditta Softech di Bologna)	Cartacei-elettronici
61.	Gestione anagrafica iscritti per organizzazione del servizio (comunicazione degli stessi al gestore in appalto del servizio) (il personale comunale incaricato fa parte dell'ISTITUZIONE SISTeR in essere dall'1.9.06).			ISTITUZIONE SISTER Refezione trasporto parascolastici	Ditta esterna che gestisce tali servizi (Società Dolce di Bologna), ditta esterna che fornisce i software SOSIA, Gradus, Sportello (Ditta Softech di Bologna)	Cartacei-elettronici
62.	Gestione anagrafica utenti finalizzata alla bollettazione dei servizi (Indirizzi e criteri per l'applicazione delle rette relative ai servizi educativi e scolastici delib. C.C. n. 7 del 4.02.09) (il personale comunale incaricato fa parte dell'ISTITUZIONE SISTeR in essere dall'1.9.06).			ISTITUZIONE SISTER Refezione, Trasporto scol., parascolastici	Ditta esterna che gestisce tali servizi (Società Dolce di Bologna), ditta esterna che fornisce i software SOSIA, Gradus, Sportello (Ditta Softech di Bologna), ditta AGERC di Cesenatico (FO) per recupero crediti	Cartacei-elettronici
63.	Per il servizio di refezione scolastica: ricevimento certificati medici relativi a diete speciali legate a patologie (intolleranze alimentari, allergie) e richieste di diete speciali per motivi religiosi (il personale comunale incaricato fa parte dell'ISTITUZIONE SISTeR in essere dall'1.9.06).	X		ISTITUZIONE SISTER Refezione, Trasporto scol., parascolastici, centri estivi	ASL Bologna, Ditta esterna che gestisce tali servizi (Società Dolce di Bologna), Istituto Comprensivo di Castenaso (personale che effettua servizio distribuzione pasti), Cooperativa Pictor (personale che effettua servizio distribuzione pasti)	Cartacei-elettronici

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
64.	Raccolta dati richiedenti al fine dell'ammissione degli stessi ai laboratori.			AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Educativi e Scolastici, Sport – Laboratori extrascolastici		Cartacei-elettronici
65.	Raccolta domande provenienti dagli Istituti Scolastici, alla quale è allegata la scheda individuale, la diagnosi funzionale e il progetto di integrazione per ciascun alunno, al fine dell'approvazione degli interventi da parte del Comune, in relazione alle risorse disponibili.	X		AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Educativi e Scolastici, Sport – Sostegno alunni portatori di handicap	Ditta esterna che gestisce in appalto tali servizi comunali	Cartacei-elettronici
66.	Raccolta domande Associazioni ai fini dell'iscrizione all'Albo comunale delle Associazioni di promozione sociale, istituito con atto di C.C. n. 53 del 2006.			AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Sociali, Politiche Abitative, Sanità		Cartacei-elettronici
67.	Raccolta domande per accedere ai contributi regionali per disabili gravi, previsti dalla L.R. 29/97 agli artt. 9 e 10	X		AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Sociali, Politiche Abitative, Sanità	Ufficio di Piano del Distretto Pianura Est presso Comune S.Pietro in Casale	Cartacei
68.	Segnalazione situazioni di minori, anche disabili, seguiti dal Servizio Sociale comunale ai fini della loro partecipazione alla vacanze per ragazzi ed handicap sia minori sia handicap	X		AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Sociali, Politiche Abitative, Sanità	Ufficio di Piano del Distretto Pianura Est presso Comune S.Pietro in Casale	Cartacei -elettronici
69.	Raccolta dati Società Sportive e gruppi amatoriali richiedenti ai fini della predisposizione quadro assegnazioni in base a criteri di priorità (Criteri approvati dalla Consulta Comunale Sportiva).			AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Educativi e Scolastici, Sport – Assegnazione Spazi Impianti Sportivi Comunali		Cartacei-elettronici
70.	Raccolta domande per la fruizione di contributi scolastici erogati dalla Provincia di Bologna (borse di studio, fornitura gratuita libri di testo L.R. 26/2001) inviate da Istituti Scolastici e istruttoria delle stesse, tramite verifica dei requisiti di reddito, al fine dell'erogazione del beneficio agli aventi diritto			AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Educativi e Scolastici, Sport – Borse di studio- fornitura gratuita e semigratuita libri di testo	Banca dati INPS, Provincia di Bologna, Regione Emilia Romagna, Istituto Comprensivo di Castenaso, altri Istituti scolastici	Cartacei-elettronici

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
71.	Gestione anagrafica Società Sportive e Gruppi amatoriali ai fini della bollettazione relativa alla fruizione degli spazi.			AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Educativi e Scolastici, Sport – Assegnazione Spazi Impianti Sportivi Comunali		Cartacei-elettronici
72.	Raccolta domande Società Sportive richiedenti al fine dello svolgimento dell'istruttoria ed erogazione contributi ad aventi diritto.			AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Educativi e Scolastici, Sport – Assegnazione contributi per attività sportiva giovanile		Cartacei-elettronici
73.	Esame singole domande con dati richiedenti al fine della erogazione del beneficio.			AREA SERVIZI ALLA PERSONA E COMUNICAZIONE Servizi Educativi e Scolastici, Sport – Assegnazione contributi per attività sportiva e ricreativa		Cartacei-elettronici
74.	Gestione anagrafica dati legali rappresentanti Società Sportive del territorio al fine della convocazione assemblee della Consulta ed altre comunicazioni che li riguardano (Modifica Regolamento Consulta Comunale Sportiva delib. C.C. n. 3 del 30.1.2008).			AREA SERVIZI ALLA PERSONA/COMUNICAZIONE Segreteria consulta comunale sportiva		Cartacei-elettronici
75.	Dati anagrafici di tutte le pratiche edilizie (DIA, permessi di costruire, pratiche per il cemento armato, conformità edilizie) dei seguenti soggetti: intestatari della pratica, tecnici incaricati dai privati, ditte che eseguono i lavori.			AREA TECNICA - U.O. EDILIZIA - PATRIMONIO - SUAP	AGENZIA DELLE ENTRATE – MINISTERO DELLE FINANZE	Elettronici
76.	Dichiarazioni di conformità impianti ai sensi del Decreto 37/2008			AREA TECNICA - U.O. EDILIZIA - PATRIMONIO - SUAP	Camera di Commercio di Iscrizione delle Ditte Esecutrici	Cartaceo
77.	Dati anagrafici di cittadini in ambito di partecipazione al procedimento amministrativo (richieste di visure pratiche e di accesso agli atti).			AREA TECNICA - U.O. EDILIZIA - PATRIMONIO - SUAP		Cartacei-elettronici
78.	Dichiarazioni sostitutive di notorietà in materia di antimafia (per condoni edilizi).			AREA TECNICA - U.O. EDILIZIA - PATRIMONIO - SUAP		Cartacei-elettronici
79.	Copie di certificati Camera di Commercio (pratiche per agricoltori – ditte esecutrici lavori edili)			AREA TECNICA - U.O. EDILIZIA - PATRIMONIO - SUAP		Cartacei-elettronici

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
80.	Copie Durc Ditte Esecutrici Lavori Edili			AREA TECNICA – U.O. EDILIZIA - PATRIMONIO - SUAP		Cartacei-elettronici
81.	Dati anagrafici di tutte le pratiche edilizie ricevute dalla U.O.			AREA TECNICA – U.O. EDILIZIA - PATRIMONIO - SUAP	PROVINCIA, ARPA, AUSL, VV.FF. , REGIONE EMILIA ROMAGNA, SOPRINTENDENZA, HERA, ENEL Società ICA di La Spezia, Provincia di Bologna	Cartacei-elettronici
82.	Dati identificativi richiedenti nulla osta installazione insegne sul territorio			AREA TECNICA – U.O. EDILIZIA - PATRIMONIO - SUAP	Prefettura Comando VV.FF	Cartacei-elettronici
83.	Copia diffide esercizio attività emesse in assenza del parere e/o certificato prevenzione incendi da parte del Comando Prov.le di Vigili del Fuoco			AREA TECNICA – U.O. EDILIZIA - PATRIMONIO - SUAP		Cartacei-elettronici
84.	Relazione Abusi edilizi ricevuti sul territorio comunale			AREA TECNICA – U.O. EDILIZIA - PATRIMONIO - SUAP	Provincia di Bologna, Giunta Regionale, Procura della Repubblica, Ministero delle Infrastrutture e dei Trasporti	Cartacei-elettronici
85.	Raccolta di atti notarili per vendita di immobili/terreni (dati anagrafici dei sottoscrittori).			AREA TECNICA - U.O. EDILIZIA - PATRIMONIO - SUAP		Cartacei-elettronici
86.	Dati portatori handicap per concessione contributi regionali legge 13/1989.			AREA TECNICA - U.O. EDILIZIA - PATRIMONIO - SUAP	REGIONE EMILIA ROMAGNA, INAIL	Cartacei-elettronici
87.	Dati anagrafici componenti CQAP (ex-Commissione Edilizia)			AREA TECNICA - U.O. EDILIZIA - PATRIMONIO - SUAP		Cartacei-elettronici
88.	Dati anagrafici fornitori/ ditte di manutenzione.			AREA TECNICA – LAVORI PUBBLICI	Osservatorio lavori pubblici, ARPA-USL Sportello Unico Imprese	Cartacei-elettronici
89.	Dati contratti pubblici di lavori, servizi e forniture relativi alla ditta aggiudicataria, esecutrice, eventuali sub-appaltatori e progettisti			AREA TECNICA – LAVORI PUBBLICI	SITAR – Sistema Informativo Telematico della Regione E.R.	Cartacei-elettronici
90.	Trasmissione dati contratti pubblici di lavori, servizi e forniture relativi alla ditta aggiudicataria, esecutrice dei lavori, ed eventuali sub-appalti.			AREA TECNICA – LAVORI PUBBLICI	Autorità per la vigilanza sui contratti pubblici di lavori, servizi e forniture	Cartacei-elettronici
91.	Dati anagrafici per richiesta dei Durc delle ditte aggiudicatarie esecutrici e subappaltatrici			AREA TECNICA	Sportello Unico (Inps, Inail, Ceda, CME)	Cartacei-elettronici
92.	Dati anagrafici altre attività economiche (pubblici esercizi, barbieri, parrucchieri, estetisti, benzinai, gelaterie, gastronomie, pasticcerie, rosticcerie, pasta fresca, pizzerie d'asporto, imprese artigiane etc.).	X		AREA TECNICA – U.O. COMMERCIO / SERVIZI AMMINISTRATIVI	AUSL BOLOGNA	Cartacei-elettronici

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
93.	Richiesta certificati casellari giudiziali e carichi pendenti (strutture ricettive, pubblici esercizi, autorizzazioni di p.s. , facchini)		X	AREA TECNICA – U.O. COMMERCIO / SERVIZI AMMINISTRATIVI	PROCURA DELLA REPUBBLICA C/O TRIBUNALE DI BOLOGNA	Cartacei-elettronici
94.	Strutture ricettive (affittacamere, bed & breakfast)		X	AREA TECNICA – U.O. COMMERCIO / SERVIZI AMMINISTRATIVI	PROVINCIA DI BOLOGNA	Cartacei-elettronici
95.	Dati anagrafici dei richiedenti l'effettuazione di manifestazioni varie, spettacoli viaggiatori, fiere, sagre, fuochi d'artificio)		X	AREA TECNICA – U.O. COMMERCIO / SERVIZI AMMINISTRATIVI	Questura di Bologna	Cartacei-elettronici
96.	Dati anagrafici dei richiedenti il rilascio di patenti per l'utilizzo di gas tossici		X	AREA TECNICA – U.O. COMMERCIO / SERVIZI AMMINISTRATIVI	U.S.L.	Cartacei-elettronici
97.	Dati anagrafici dei richiedenti l'autorizzazione alla vendita di cose usate e antiche		X	AREA TECNICA – U.O. COMMERCIO / SERVIZI AMMINISTRATIVI	Questura di Bologna	Cartacei-elettronici
98.	Dati contratti pubblici di lavori, servizi e forniture relativi alla ditta aggiudicataria, esecutrice dei lavori, ed eventuali sub-appalti.			AREA TECNICA – U.O. SERVIZI AMBIENTALI	Sportello unico previdenziale (INPS-INAIL-C.M.E. CEDA); SITAR – Sistema Informativo Telematico della Regione E.R.;	Cartacei-elettronici
99.	Dati anagrafici per compilazione contratto di comodato gratuito per la successiva consegna di compostiere domestiche			AREA TECNICA – U.O. SERVIZI AMBIENTALI		Cartacei-elettronici
100.	Domande di accesso agli atti per visura pratiche			AREA TECNICA – U.O. SERVIZI AMBIENTALI		Cartacei-elettronici
101.	Dati anagrafici relativi a schede identificative di impianti termici			AREA TECNICA – U.O. SERVIZI AMBIENTALI	UFFICIO RISANAMENTO ATMOSFERICO C/O PROVINCIA DI BOLOGNA	Cartacei-elettronici
102.	Dati anagrafici richiedenti il contributo per la trasformazione di impianti auto da benzina a gpl/metano			AREA TECNICA – U.O. SERVIZI AMBIENTALI	Regione Emilia Romagna	Cartacei-elettronici

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
103.	Dati anagrafici di cittadini che utilizzano prodotti larvicidi.			AREA TECNICA – U.O. SERVIZI AMBIENTALI	Centro Agricoltura Ambiente di Crevalcore (direzione tecnica del U.O. di disinfestazione- assistenza tecnica-scientifica)	Cartacei-elettronici
104.	Dati anagrafici intestatari TARSU (legato al Premio ai conferitori in SEA)			AREA TECNICA – U.O. SERVIZI AMBIENTALI		Cartacei-elettronici
105.	Dati anagrafici di cittadini che presentano osservazioni a piani particolareggiati e a piani urbanistici			AREA TECNICA – PIANIFICAZIONE TERRITORIALE	REGIONE EMILIA ROMAGNA	Cartacei-elettronici
106.	Dati anagrafici professionisti progettisti incaricati.			AREA TECNICA – LAVORI PUBBLICI	PROVINCIA DI BOLOGNA Osservatorio lavori pubblici, ARPA-USL	Cartacei-elettronici
107.	Dati anagrafici ditte partecipanti alle gare/subappaltatori (relative dichiarazioni antimafia e pronunce di condanna penale).			AREA TECNICA – LAVORI PUBBLICI	Sportello Unico Imprese Osservatorio lavori pubblici, ARPA-USL	Cartacei-elettronici
108.	Dati anagrafici ditte esercenti commercio fisso e su area pubblica (ambulanti)	X		AREA TECNICA – U.O. COMMERCIO / SERVIZI AMMINISTRATIVI	Agenzia delle Entrate – Ministero delle Finanze (anagrafe tributaria) Regione Emilia Romagna CCIAA	Cartacei-elettronici
109.	Dati anagrafici (e relativi casellari giudiziali) esercenti l'attività di facchino.	X		AREA TECNICA – U.O. COMMERCIO / SERVIZI AMMINISTRATIVI		Cartacei-elettronici
110.	Copie certificati Camera di Commercio.			AREA TECNICA – U.O. COMMERCIO / SERVIZI AMMINISTRATIVI		Cartacei-elettronici
111.	Dati anagrafici di cittadini in ambito di partecipazione al procedimento amministrativo (richieste di visure pratiche e di accesso agli atti).			AREA TECNICA – U.O. COMMERCIO / SERVIZI AMMINISTRATIVI		Cartacei-elettronici
112.	Dati anagrafici di fornitori/ditte di manutenzione.			AREA TECNICA – U.O. SERVIZI AMBIENTALI		Cartacei-elettronici
113.	Dati anagrafici di professionisti incaricati.			AREA TECNICA – U.O. SERVIZI AMBIENTALI		Cartacei-elettronici
114.	Dati anagrafici per iniziativa “Un albero per ogni bambino” Legge 113/1992.			AREA TECNICA – U.O. SERVIZI AMBIENTALI		Cartacei-elettronici
115.	Dati anagrafici di tutte le pratiche del U.O. Ambiente (autorizzazioni allo scarico, abbattimento alberi, etc).			AREA TECNICA – U.O. SERVIZI AMBIENTALI	HERA BOLOGNA	Cartacei-elettronici

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
116.	Dati anagrafici dei professionisti incaricati.			AREA TECNICA – PIANIFICAZIONE TERRITORIALE		Cartacei-elettronici
117.	Dati anagrafici di cittadini in ambito di partecipazione al procedimento amministrativo (richieste di visura pratiche e di accesso agli atti).			AREA TECNICA – PIANIFICAZIONE TERRITORIALE		Cartacei-elettronici
118.	Dati anagrafici affittuari immobili comunali.			COMUNE DI CASTENASO – UFFICIO CASA		Cartacei-elettronici
119.	Gestione e archiviazione contravvenzioni amm.ve C.d.S. e Regolamenti Comunali.	X		POLIZIA MUNICIPALE – Servizio Polizia Municipale		Cartacei-elettronici
120.	Gestione e archiviazione contravvenzioni amm.ve per violazioni normativa sul commercio.	X		POLIZIA MUNICIPALE – Servizio Polizia Municipale		Cartacei-elettronici
121.	Gestione e archiviazione contravvenzioni amm.ve per violazioni normativa vigente.	X		POLIZIA MUNICIPALE – Servizio Polizia Municipale		Cartacei-elettronici
122.	Gestione e archiviazione Accertamenti e Informazioni.			POLIZIA MUNICIPALE – Servizio Polizia Municipale		Cartacei-elettronici
123.	Gestione e archiviazione dati dei conducenti i veicoli controllati. (Socrate).	X		POLIZIA MUNICIPALE – Servizio Polizia Municipale		Cartacei-elettronici
124.	Gestione e archiviazione rapporti di infortunistica stradale.	X	X	POLIZIA MUNICIPALE – Servizio Polizia Municipale		Cartacei-elettronici
125.	Gestione e archiviazione Autorizzazioni Persone invalide.	X		POLIZIA MUNICIPALE – Servizio Polizia Municipale		Cartacei-elettronici
126.	Gestione e archiviazione Autorizzazioni Pubblicità temporanea e fonica.	X		POLIZIA MUNICIPALE – Servizio Polizia Municipale		Cartacei-elettronici
127.	Gestione e archiviazione Autorizzazioni TOSAP temporanea.	X		POLIZIA MUNICIPALE – Servizio Polizia Municipale		Cartacei-elettronici
128.	Gestione e archiviazione Polizia Giudiziaria (CdS, Edilizia, PS, CP, CPP).		X	POLIZIA MUNICIPALE – Servizio Polizia Municipale		Cartacei-elettronici
129.	Gestione e archiviazione pratiche personale dipendente.	X		POLIZIA MUNICIPALE – Servizio Polizia Municipale		Cartacei-elettronici
130.	Gestione registrazione telefonate con archiviazione (max 10gg.), nel rispetto delle prescrizioni del Garante.	X		POLIZIA MUNICIPALE – Servizio Polizia Municipale		Elettronici
131.	Gestione archiviazione immagini del sistema di videosorveglianza (max 7gg.), nel rispetto delle prescrizioni del Garante.	X	X	POLIZIA MUNICIPALE – Servizio Polizia Municipale		Elettronici

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
132.	Gestione giuridica del rapporto di lavoro (ivi compresi procedimenti di: mutamento mansioni per inidoneità fisica, infermità per causa di servizio, congedi parentali, aspettative, permessi L.104/92, infortuni sul lavoro, procedimenti disciplinari, ecc.)	X		SEGRETARIO Sviluppo organizzativo del personale	GENERALE e politiche	Cartacei-elettronici
133.	Gestione economica del rapporto di lavoro dipendente (ivi compresi: assegni familiari, prestiti pluriennali, ritenute sindacali, ecc.)	X		SEGRETARIO Sviluppo organizzativo del personale	GENERALE e politiche	Ditta esterna che fornisce il software gestionale Cartacei-elettronici
134.	Gestione ed elaborazione dati stipendiali personale dipendente ivi compresi i redditi assimilati a lavoro dipendente (amministratori, componenti commissioni, co.co.co).	X		SEGRETARIO Sviluppo organizzativo del personale	GENERALE e politiche	Ditta esterna che fornisce il software gestionale Cartacei-elettronici
135.	Adempimenti fiscali, assicurativi, contributivi, TFR, ecc.	X		SEGRETARIO Sviluppo organizzativo del personale	GENERALE e politiche	Ditta esterna che fornisce software gestionale Cartacei-elettronici
136.	Gestione presenze/assenze	X		SEGRETARIO Sviluppo organizzativo del personale	GENERALE e politiche	Ditta esterna che fornisce software gestionale Cartacei-elettronici
137.	Pratiche previdenziali, sistemazioni contributive, ricongiunzioni, riscatti, ecc	X		SEGRETARIO Sviluppo organizzativo del personale	GENERALE e politiche	Ditta esterna: incarico annuale per le pratiche previdenziali Cartacei-elettronici
138.	Controlli sanitari (D.Lgs.81/2008, inidoneità, nuove assunzioni ecc.).	X		SEGRETARIO Sviluppo organizzativo del personale	GENERALE e politiche	Medico competente, Ditta esterna (verifica 81/2008) Cartacei-elettronici
139.	Procedure concorsuali/selettive (anche L.68/99 –disabili)	X		SEGRETARIO Sviluppo organizzativo del personale	GENERALE e politiche	Cartacei-elettronici
140.	Lavoro interinale.	X		SEGRETARIO Sviluppo organizzativo del personale	GENERALE e politiche	Cartacei-elettronici
141.	Relazioni sindacali.	X		SEGRETARIO Sviluppo organizzativo del personale	GENERALE e politiche	Cartacei-elettronici

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
142.	Statistiche varie inerenti dotazione organica , costi del personale, permessi sindacali, ecc.			SEGRETARIO GENERALE Sviluppo organizzativo e politiche del personale		Cartacei-elettronici
143.	Elaborazione atti di difesa/costituzione in giudizio dell'ente.			SEGRETARIO GENERALE Consulenza giuridica, contenzioso, gare e contratti		Cartacei-elettronici
144.	Gestione contenzioso stragiudiziale (accordi di transazione e comunicazioni).			SEGRETARIO GENERALE Consulenza giuridica, contenzioso, gare e contratti		Cartacei-elettronici
145.	Elaborazione contratti/disciplinari di incarico. Trasmissione dati collaboratori esterni (incarichi professionali)			SEGRETARIO GENERALE Consulenza giuridica, contenzioso, gare e contratti	Ministero Funzione Pubblica/Anagrafe delle Prestazioni	Cartacei-elettronici
146.	Trasmissione dati anagrafici ditte aggiudicatarie di lavori pubblici, servizi e forniture.			SEGRETARIO GENERALE Consulenza giuridica, contenzioso, gare e contratti	Ufficio Territoriale del Governo - Bologna	Cartacei-elettronici
147.	Richiesta certificazioni (casellario e carichi pendenti) di ditte aggiudicatarie di lavori pubblici, servizi e forniture.			SEGRETARIO GENERALE Consulenza giuridica, contenzioso, gare e contratti	Procura della Repubblica c/o Tribunale di Bologna	Cartacei-elettronici
148.	Gestione dati anagrafici di studi legali.			SEGRETARIO GENERALE Consulenza giuridica, contenzioso, gare e contratti		Cartacei-elettronici
149.	Dati anagrafici per richiesta dei Durc delle ditte aggiudicatarie di lavori pubblici, servizi e forniture.			SEGRETARIO GENERALE Consulenza giuridica, contenzioso, gare e contratti	Sportello Unico (Inps, Inail, Ceda, CME)	Cartacei-elettronici

Data di aggiornamento: 15/03/2010

Tavola 4. Elenco dei trattamenti: descrizione degli strumenti utilizzati

Identificativo del trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
1.	Gestione protocollo comunale.	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
2.	Sito Internet-Periodico comunale, comunicati stampa, mailing list , customer satisfaction (attività in fase di preparazione).	Server di rete e armadio	Personal Computer e manualmente	Intranet
3.	Contrassegni invalidi, denunce infortuni, denunce cessione alloggi,licenze caccia/pesca, ritiro richieste iscrizione servizi comunali.	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
4.	Gestione reclami.	Server di rete e armadio	Personal Computer e manualmente	Intranet
5.	Raccolta originali atti (delibere, determine, ordinanze), convocazioni giunta e consiglio.	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
6.	Notifiche, albi, difensore civico, mediatore sociale.	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
7.	Gestione anagrafe-stato civile -leva –elettorale.	Server di rete e armadio con chiave	Manualmente	Intranet
8.	Tenuta registri.	Armadio con chiave	Manualmente	
9.	Rilascio certificati.	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
10.	Documentazione amministrativa (autentiche, copie conformi).	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
11.	Statistiche.	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
12.	Procedimenti elettorali.	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
13.	Tenuta albi (Presidenti, scrutatori, Giudici popolari).	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
14.	Gestione dati trasmessi da pompe funebri in relazione al rilascio autorizzazione trasporto salme e trasporto e cremazione.	Server di rete e armadio	Personal Computer e manualmente	Intranet
15.	Gestione dati trasmessi da pompe funebri in relazione al rilascio autorizzazione trasporto salme e trasporto e cremazione.	Server di rete e armadio	Personal Computer e manualmente	Intranet
16.	Abbonamenti agevolati per mezzi pubblici: assistenza ai richiedenti per compilazione modulo per concessione abbonamento agevolato.	Server di rete e armadio	Personal Computer e manualmente	Intranet
17.	Gestione dati di tutti i beneficiari per anno solare al fine della compilazione dell'Albo dei beneficiari di provvidenze economiche (DPR 7.4.2000 n. 118).	Server di rete e armadio	Personal Computer e manualmente	Intranet
18.	Raccolta dati richiedenti al momento della domanda di iscrizione al servizio.	Server di rete e armadio	Personal Computer e manualmente	Intranet
19.	Elaborazione atti di difesa/costituzione in giudizio dell'ente.	Server di rete e armadio	Personal Computer e manualmente	Intranet
20.	Gestione contenzioso stragiudiziale (accordi di transazione e comunicazioni).	Server di rete e armadio	Personal Computer e manualmente	Intranet
21.	Elaborazione contratti/disciplinari di incarico. Trasmissione dati collaboratori esterni (incarichi professionali)	Server di rete e armadio	Personal Computer e manualmente	Intranet

Identificativo del trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
22.	Trasmissione dati anagrafici ditte aggiudicatarie di lavori pubblici, servizi e forniture.	Server di rete e armadio	Personal Computer e manualmente	Intranet
23.	Richiesta certificazioni (casellario e carichi pendenti) di ditte aggiudicatarie di lavori pubblici, servizi e forniture.	Server di rete e armadio	Personal Computer e manualmente	Intranet
24.	Gestione dati anagrafici di studi legali.	Server di rete e armadio	Personal Computer e manualmente	Intranet
25.	Dati anagrafici per richiesta dei Durc delle ditte aggiudicatarie di lavori pubblici, servizi e forniture ai soli fini della stipulazione del contratto d'appalto	Server di rete e armadio	Personal Computer e manualmente	Intranet
26.	Calcolo relativo alla minore contribuzione di ogni utente del servizio nido in base alla propria quota agevolata rispetto alla retta massima, al fine della compilazione dell'Albo dei beneficiari di provvidenze economiche (DPR 7.4.2000 n. 118).	Armadio	Manualmente	
27.	Gestione dati di tutti i beneficiari per anno solare al fine della compilazione dell'Albo dei beneficiari di provvidenze economiche (DPR 7.4.2000 n. 118).	Server di rete e armadio	Personal Computer e manualmente	Intranet
28.	Gestione dati di tutti i beneficiari per anno solare per rendicontazione contributi straordinari (art. 158 Dlgs. 267/2000) e per compilazione dell'Albo dei beneficiari di provvidenze economiche (DPR 7.4.2000 n. 118).	Server di rete e armadio	Personal Computer e manualmente	Intranet
29.	Periodico comunale, comunicati stampa, mailing list	Server di rete e armadio	Personal Computer e manualmente	Intranet
30.	Gestione anagrafica contribuenti Imposta comunale sugli immobili, Tassa Rifiuti Solidi Urbani, Tassa Occupazione Spazi ed Aree Pubbliche.	Server di rete e armadio	Personal Computer e manualmente	Intranet
31.	Gestione dati relativi alla situazione reddituale di contribuenti che fanno richiesta di particolari agevolazioni in materia di tributi locali quali I.C.I. e T.A.R.S.U.	Server di rete e armadio	Personal Computer e manualmente	Intranet
32.	Gestione dati relativi alla situazione sanitaria (presenza all'interno del nucleo familiare di portatori di handicap) di contribuenti che fanno richiesta di particolari agevolazioni in materia di I.C.I.	Server di rete e armadio	Personal Computer e manualmente	Intranet
33.	Gestione anagrafica concessionari posizioni cimiteriali e defunti.	Server di rete e armadio	Personal Computer e manualmente	Intranet
34.	Gestione dati relativi a Fornitori/Prestatori di servizi/incaricati/Personale Dipendente del Comune di Castenaso (anagrafica persone fisiche/giuridiche; coordinate bancarie; gestione fatture).	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet

Identificativo del trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
35.	Tenuta presso l'Ufficio ragioneria di atti (determinazioni/delibere) rilevanti ai fini contabili predisposti da altri servizi/settori e contenenti anagrafiche di soggetti percettori di contributi, ricoveri in istituti convenzionali ecc.	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
36.	Gestione di dati relativi ad alcuni fornitori (ragione sociale, indirizzo, n° di telefono e fax, coordinate bancarie, ecc. dei fornitori del Servizio Economato).	Server di rete e armadio	Personal Computer e manualmente	Intranet
37.	Gestione dati relativi ai sinistri avvenuti nel territorio del Comune e inerenti le Polizze Assicurative Comunali (ad es. RCT/O, RC Auto, Infortuni Alunni,...).	Server di rete e armadio	Personal Computer e manualmente	Intranet
38.	Gestione di dati relativi ai dipendenti aventi diritto al vestiario, come – ad esempio – certificati medici che implicano l'esonero dall'utilizzo di calzature antinfortunistiche.	Server di rete e armadio	Personal Computer e manualmente	Intranet
39.	Gestione dati relativi agli oggetti smarriti (il Servizio Economato riceve e custodisce i verbali di rinvenimento redatti dalla Polizia Municipale e redige i verbali di riconsegna al proprietario o al ritrovatore).	Server di rete e armadio	Personal Computer e manualmente	Intranet
40.	Aggiornamento anagrafica fornitori/clienti	Server di rete e armadio	Personal Computer e manualmente	Intranet
41.	Osservatorio provinciale per la registrazione degli accessi sia diretti sia telefonici allo Sportello Sociale	Server di rete	Personal Computer	Intranet
42.	Servizio Assistenza Domiciliare (SAD): gestione anagrafica utenti per accesso al servizio (tramite programma informatico GARSIA); gestione utenti per bollettazione rette (tramite programma SOSIA); gestione cartelle individuali per utente (contengono anche dati sensibili).	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
43.	Orti: gestione anagrafica per assegnazione e relativa bollettazione retta annuale (tramite programma SOSIA).	Server di rete e armadio	Personal Computer e manualmente	Intranet
44.	Abbonamenti agevolati per mezzi pubblici: assistenza ai richiedenti per compilazione modulo per concessione abbonamento agevolato sia per studenti che anziani e disabili	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet

Identificativo del trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
45.	Politiche abitative: gestione anagrafica richiedenti ed assegnatari alloggi ERP, appartamenti Servizio Pronto Emergenza abitativa ed alloggi a canoni agevolati; gestione abitativa (contratto, importo affitto, eventuale provvedimento sfratto, dimensioni e caratteristiche di idoneità dell'alloggio), bollettazione utenti Pronto Emergenza Abitativa; predisposizione graduatorie pubbliche per richiedenti alloggi ERP o a canone agevolato.	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
46.	Raccolta domande e relativa istruttoria ai fini della concessione del contributo per l'affitto (ai sensi della L. 431/98, della L.R. n. 24/2001)	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
47.	Centro Accoglienza Extracomunitari: gestione anagrafica (oltre ai dati anagrafici, nazionalità, permesso/carta di soggiorno valida), condizioni sociali e sanitarie, lavorative e abitative dei richiedenti per assegnazione posto letto; gestione utenti per bollettazione rette mensili (tramite programma SOSIA).	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
48.	Contributi/benefici economici: gestione richiedenti/utenti (persone fisiche e associazioni) contributi comunali (una- tantum, esenzioni ticket, contributi per handicap, contributi per integrazione rette di ricovero in struttura);riduzioni /esenzioni rette scolastiche e per l'Asilo Nido; gestione richiedenti assegno per nucleo numeroso e per maternità (Legge 448/98 artt.65-66); gestione utenti per contributo regionale a sostegno dell'affitto, il relativo contributo viene calcolato tramite programma informatico regionale.	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
49.	Invalidità civili : gestione pratiche utenti per concessione provvidenze economiche; gestione dichiarazioni di responsabilità che i titolari di accompagnamento sono tenuti a fare annualmente.	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
50.	Interventi in favore di anziani non-autosufficienti (L.R 5/94): gestione utenti per accesso alla rete dei servizi socio-sanitari integrati (tramite programma informatico GARSIA).	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet

Identificativo del trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
51.	Certificazioni ISEE: attestazione condizioni economiche ai fini della concessione di contributi ed agevolazioni tariffarie di vario tipo nonché per l'ammissione ai vari servizi che lo prevedono fra i requisiti di accesso (calcolata ai sensi D.Lgs n. 109/98 e successive modificazioni ed integrazioni), tramite programma INPS.	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
52.	Raccolta dati dei nuclei familiari richiedenti il servizio, attraverso il modulo di domanda e dichiarazione sostitutiva unica finalizzata al calcolo dell'indicatore ISEE (facoltativa), al fine della formazione delle graduatorie di ammissione (Regolamento comunale servizi educativi per la prima infanzia delib. C.C. n. 6 del 4.02.2009) e della successiva comunicazione agli interessati dell'ammissione/non ammissione al nido.	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
53.	Gestione anagrafica iscritti, al fine della bollettazione del servizio.	Server di rete e armadio	Personal Computer e manualmente	Intranet
54.	Raccolta schede di anamnesi per i nuovi ammessi ed inoltro delle stesse alla ASL, al fine dello svolgimento degli opportuni controlli sanitari da parte della stessa.	Server di rete e armadio	Personal Computer e manualmente	Intranet
55.	Gestione anagrafica richiedenti ed iscritti	Server di rete e armadio	Personal Computer e manualmente	Intranet
56.	Raccolta dati richiedenti al momento della domanda di iscrizione al servizio.	Server di rete e armadio	Personal Computer e manualmente	Intranet
57.	Gestione anagrafica richiedenti ed iscritti. – Gestione dati utenti Sportello d'ascolto 0-6 anni (intervento di sostegno alla genitorialità)	Armadio con chiave	Manualmente	
58.	Gestione anagrafica iscritti per organizzazione del servizio (comunicazione degli stessi al gestore in appalto del servizio).	Armadio con chiave	Manualmente	
59.	Gestione anagrafica iscritti al fine della bollettazione del servizio (Indirizzi e criteri per l'applicazione delle rette relative ai servizi educativi e scolastici delib. C.C. n. 7 del 4.02.09).	Server di rete	Personal Computer	Intranet
60.	Raccolta dati richiedenti al momento della domanda di iscrizione al servizio.	Server di rete e armadio	Personal Computer e manualmente	Intranet
61.	Gestione anagrafica iscritti per organizzazione del servizio (comunicazione degli stessi al gestore in appalto del servizio) (il personale comunale incaricato fa parte dell'ISTITUZIONE SISTeR in essere dall'1.9.06).	Server di rete e armadio	Personal Computer e manualmente	Intranet

Identificativo del trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
62.	Gestione anagrafica utenti finalizzata alla bollettazione dei servizi (Indirizzi e criteri per l'applicazione delle rette relative ai servizi educativi e scolastici delib. C.C. n. 7 del 4.02.09) (il personale comunale incaricato fa parte dell'ISTITUZIONE SISTeR in esser dall'1.9.06).	Server di rete e armadio	Personal Computer e manualmente	Intranet
63.	Per il servizio di refezione scolastica: ricevimento certificati medici relativi a diete speciali legate a patologie (intolleranze alimentari, allergie) e richieste di diete speciali per motivi religiosi (il personale comunale incaricato fa parte dell'ISTITUZIONE SISTeR in essere dall'1.9.06).	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
64.	Raccolta dati richiedenti al fine dell'ammissione degli stessi ai laboratori.	Server di rete e armadio	Personal Computer e manualmente	Intranet
65.	Raccolta domande provenienti dagli Istituti Scolastici, alla quale è allegata la scheda individuale, la diagnosi funzionale e il progetto di integrazione per ciascun alunno, al fine dell'approvazione degli interventi da parte del Comune, in relazione alle risorse disponibili.	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
66.	Raccolta domande Associazioni ai fini dell'iscrizione all'Albo comunale delle Associazioni di promozione sociale, istituito con atto di C.C. n. 53 del 2006.	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
67.	Raccolta domande per accedere ai contributi regionali per disabili gravi, previsti dalla L.R. 29/97 agli artt. 9 e 10	Server di rete e armadio con chiave	Manualmente	Intranet
68.	Segnalazione situazioni di minori, anche disabili, seguiti dal Servizio Sociale comunale ai fini della loro partecipazione alla vacanze per ragazzi ed handicap sia minori sia handicap	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
69.	Raccolta dati Società Sportive e gruppi amatoriali richiedenti ai fini della predisposizione quadro assegnazioni in base a criteri di priorità (Criteri approvati dalla Consulta Comunale Sportiva).	Server di rete e armadio	Personal Computer e manualmente	Intranet
70.	Raccolta domande per la fruizione di contributi scolastici erogati dalla Provincia di Bologna (borse di studio, fornitura gratuita libri di testo L.R. 26/2001) inviate da Istituti Scolastici e istruttoria delle stesse, tramite verifica dei requisiti di reddito, al fine dell'erogazione del beneficio agli aventi diritto	Server di rete e armadio	Personal Computer e manualmente	Intranet
71.	Gestione anagrafica Società Sportive e Gruppi amatoriali ai fini della bollettazione relativa alla fruizione degli spazi.	Server di rete e armadio	Personal Computer e manualmente	Intranet

Identificativo del trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
72.	Raccolta domande Società Sportive richiedenti al fine dello svolgimento dell'istruttoria ed erogazione contributi ad aventi diritto.	Server di rete e armadio	Personal Computer e manualmente	Intranet
73.	Esame singole domande con dati richiedenti al fine della erogazione del beneficio.	Server di rete e armadio	Personal Computer e manualmente	Intranet
74.	Gestione anagrafica dati legali rappresentanti Società Sportive del territorio al fine della convocazione assemblee della Consulta ed altre comunicazioni che li riguardano (Modifica Regolamento Consulta Comunale Sportiva delib. C.C. n. 3 del 30.1.2008).	Server di rete e armadio	Personal Computer e manualmente	Intranet
75.	Dati anagrafici di tutte le pratiche edilizie (DIA, permessi di costruire, pratiche per il cemento armato, conformità edilizie) dei seguenti soggetti: intestatari della pratica, tecnici incaricati dai privati, ditte che eseguono i lavori.	Server di rete e armadio	Personal Computer e manualmente	Intranet
76.	Dichiarazioni di conformità impianti ai sensi del Decreto 37/2008	Armadio	Manualmente	
77.	Dati anagrafici di cittadini in ambito di partecipazione al procedimento amministrativo (richieste di visure pratiche e di accesso agli atti).	Server di rete e armadio	Personal Computer e manualmente	Intranet
78.	Dichiarazioni sostitutive di notorietà in materia di antimafia (per condoni edilizi).	Server di rete e armadio	Personal Computer e manualmente	Intranet
79.	Copie di certificati Camera di Commercio (pratiche per agricoltori – ditte esecutrici lavori edili)	Server di rete e armadio	Personal Computer e manualmente	Intranet
80.	Copie Durc Ditte Esecutrici Lavori Edili	Server di rete e armadio	Personal Computer manualmente	Intranet
81.	Dati anagrafici di tutte le pratiche edilizie ricevute dalla U.O.	Server di rete e armadio	Personal Computer manualmente	Intranet
82.	Dati identificativi richiedenti nulla osta installazione insegne sul territorio	Server di rete e armadio	Personal Computer e manualmente	Intranet
83.	Copia diffide esercizio attività emesse in assenza del parere e/o certificato prevenzione incendi da parte del Comando Prov.le di Vigili del Fuoco	Server di rete e armadio	Personal Computer e manualmente	Intranet
84.	Relazione Abusi edilizi ricevuti sul territorio comunale	Server di rete e armadio	Personal Computer e manualmente	Intranet
85.	Raccolta di atti notarili per vendita di immobili/terreni (dati anagrafici dei sottoscrittori).	Server di rete e armadio	Personal Computer manualmente	Intranet
86.	Dati portatori handicap per concessione contributi regionali legge 13/1989.	Server di rete e armadio	Personal Computer e manualmente	Intranet
87.	Dati anagrafici componenti CQAP (ex-Commissione Edilizia)	Server di rete e armadio	Personal Computer e manualmente	Intranet
88.	Dati anagrafici fornitori/ ditte di manutenzione.	Server di rete e armadio	Personal Computer manualmente	Intranet
89.	Dati contratti pubblici di lavori, servizi e forniture relativi alla ditta aggiudicataria, esecutrice, eventuali sub-appaltatori e progettisti	Server di rete e armadio	Personal Computer manualmente	Intranet
90.	Trasmissione dati contratti pubblici di lavori, servizi e forniture relativi alla ditta aggiudicataria, esecutrice dei lavori, ed eventuali sub-appalti.	Server di rete e armadio	Personal computer e manualmente	intranet

Identificativo del trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
91.	Dati anagrafici per richiesta dei Durc delle ditte aggiudicatarie esecutrici e subappaltatrici	Server di rete e armadio	Personal Computer manualmente	Intranet
92.	Dati anagrafici altre attività economiche (pubblici esercizi, barbieri, parrucchieri, estetisti, benzinai, gelaterie, gastronomie, pasticcerie, rosticcerie, pasta fresca, pizzerie d'asporto, imprese artigiane etc.).	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
93.	Richiesta certificati casellari giudiziali e carichi pendenti (strutture ricettive, pubblici esercizi, autorizzazioni di p.s. , facchini)	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
94.	Strutture ricettive (affittacamere, bed & breakfast)	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
95.	Dati anagrafici dei richiedenti l'effettuazione di manifestazioni varie, spettacoli viaggiatori, fiere, sagre, fuochi d'artificio)	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
96.	Dati anagrafici dei richiedenti il rilascio di patenti per l'utilizzo di gas tossici	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
97.	Dati anagrafici dei richiedenti l'autorizzazione alla vendita di cose usate e antiche	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
98.	Dati contratti pubblici di lavori, servizi e forniture relativi alla ditta aggiudicataria, esecutrice dei lavori, ed eventuali sub-appalti.	Server di rete e armadio	Personal Computer manualmente	Intranet
99.	Dati anagrafici per compilazione contratto di comodato gratuito per la successiva consegna di compostiere domestiche	Server di rete e armadio	Personal Computer manualmente	Intranet
100.	Domande di accesso agli atti per visura pratiche	Server di rete e armadio	Personal Computer manualmente	Intranet
101.	Dati anagrafici relativi a schede identificative di impianti termici	Server di rete e armadio	Personal Computer manualmente	Intranet
102.	Dati anagrafici richiedenti il contributo per la trasformazione di impianti auto da benzina a gpl/metano	Server di rete e armadio	Personal Computer manualmente	Intranet
103.	Dati anagrafici di cittadini che utilizzano prodotti larvicidi.	Server di rete e armadio	Personal Computer manualmente	Intranet
104.	Dati anagrafici intestatari TARSU (legato al Premio ai conferitori in SEA)	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
105.	Dati anagrafici di cittadini che presentano osservazioni a piani particolareggiati e a piani urbanistici	Server di rete e armadio	Personal Computer manualmente	Intranet
106.	Dati anagrafici professionisti progettisti incaricati.	Server di rete e armadio	Personal Computer manualmente	Intranet
107.	Dati anagrafici ditte partecipanti alle gare/subappaltatori (relative dichiarazioni antimafia e pronunce di condanna penale).	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
108.	Dati anagrafici ditte esercenti commercio fisso e su area pubblica (ambulanti)	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
109.	Dati anagrafici (e relativi casellari giudiziali) esercenti l'attività di facchino.	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
110.	Copie certificati Camera di Commercio.	Server di rete e armadio	Personal Computer manualmente	Intranet

Identificativo del trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
111.	Dati anagrafici di cittadini in ambito di partecipazione al procedimento amministrativo (richieste di visure pratiche e di accesso agli atti).	Server di rete e armadio	Personal Computer manualmente	Intranet
112.	Dati anagrafici di fornitori/ditte di manutenzione.	Server di rete e armadio	Personal Computer manualmente	Intranet
113.	Dati anagrafici di professionisti incaricati.	Server di rete e armadio	Personal Computer manualmente	Intranet
114.	Dati anagrafici per iniziativa "Un albero per ogni bambino" Legge 113/1992.	Server di rete e armadio	Personal Computer manualmente	Intranet
115.	Dati anagrafici di tutte le pratiche del U.O. Ambiente (autorizzazioni allo scarico, abbattimento alberi, etc).	Server di rete e armadio	Personal Computer manualmente	Intranet
116.	Dati anagrafici dei professionisti incaricati.	Server di rete e armadio	Personal Computer manualmente	Intranet
117.	Dati anagrafici di cittadini in ambito di partecipazione al procedimento amministrativo (richieste di visura pratiche e di accesso agli atti).	Server di rete e armadio	Personal Computer manualmente	Intranet
118.	Dati anagrafici affittuari immobili comunali.	Server di rete e armadio	Personal Computer manualmente	Intranet
119.	Gestione e archiviazione contravvenzioni amm.ve C.d.S. e Regolamenti Comunali.	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
120.	Gestione e archiviazione contravvenzioni amm.ve per violazioni normativa sul commercio.	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
121.	Gestione e archiviazione contravvenzioni amm.ve per violazioni normativa vigente.	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
122.	Gestione e archiviazione Accertamenti e Informazioni.	Server di rete e armadio	Personal Computer manualmente	Intranet
123.	Gestione e archiviazione dati dei conducenti i veicoli controllati. (Socrate).	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
124.	Gestione e archiviazione rapporti di infortunistica stradale.	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
125.	Gestione e archiviazione Autorizzazioni Persone invalide.	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
126.	Gestione e archiviazione Autorizzazioni Pubblicità temporanea e fonica.	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
127.	Gestione e archiviazione Autorizzazioni TOSAP temporanea.	Server di rete e armadio con chiave	Personal Computer e manualmente	Intranet
128.	Gestione e archiviazione Polizia Giudiziaria (CdS, Edilizia, PS, CP, CPP).	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
129.	Gestione e archiviazione pratiche personale dipendente.	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
130.	Gestione registrazione telefonate con archiviazione (max 10gg.), nel rispetto delle prescrizioni del Garante.	Server di rete e armadio con chiave	Personal Computer	Intranet
131.	Gestione archiviazione immagini del sistema di videosorveglianza (max 7gg.), nel rispetto delle prescrizioni del Garante.	Server di rete e armadio con chiave	Personal Computer	Intranet

Identificativo del trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
132.	Gestione giuridica del rapporto di lavoro (ivi compresi procedimenti di: mutamento mansioni per inidoneità fisica, infermità per causa di servizio, congedi parentali, aspettative , permessi L.104/92, infortuni sul lavoro, procedimenti disciplinari, ecc.)	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
133.	Gestione economica del rapporto di lavoro dipendente (ivi compresi: assegni familiari, prestiti pluriennali, ritenute sindacali, ecc.)	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
134.	Gestione ed elaborazione dati stipendiali personale dipendente ivi compresi i redditi assimilati a lavoro dipendente (amministratori, componenti commissioni, co.co.co).	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
135.	Adempimenti fiscali , assicurativi, contributivi, TFR, ecc.	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
136.	Gestione presenze/assenze	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
137.	Pratiche previdenziali, sistemazioni contributive, ricongiunzioni, riscatti, ecc	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
138.	Controlli sanitari (D.Lgs.81/2008, inidoneità, nuove assunzioni ecc.).	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
139.	Procedure concorsuali/selettive (anche L.68/99 –disabili)	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
140.	Lavoro interinale.	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
141.	Relazioni sindacali.	Server di rete e armadio con chiave	Personal Computer manualmente	Intranet
142.	Statistiche varie inerenti dotazione organica , costi del personale, permessi sindacali, ecc.	Server di rete e armadio	Personal Computer manualmente	Intranet
143.	Elaborazione atti di difesa/costituzione in giudizio dell'ente.	Server di rete e armadio	Personal Computer manualmente	Intranet
144.	Gestione contenzioso stragiudiziale (accordi di transazione e comunicazioni).	Server di rete e armadio	Personal Computer manualmente	Intranet
145.	Elaborazione contratti/disciplinari di incarico. Trasmissione dati collaboratori esterni (incarichi professionali)	Server di rete e armadio	Personal Computer manualmente	Intranet
146.	Trasmissione dati anagrafici ditte aggiudicatarie di lavori pubblici, servizi e forniture.	Server di rete e armadio	Personal Computer manualmente	Intranet
147.	Richiesta certificazioni (casellario e carichi pendenti) di ditte aggiudicatarie di lavori pubblici, servizi e forniture.	Server di rete e armadio	Personal Computer manualmente	Intranet
148.	Gestione dati anagrafici di studi legali.	Server di rete e armadio	Personal Computer manualmente	Intranet
149.	Dati anagrafici per richiesta dei Durc delle ditte aggiudicatarie di lavori pubblici, servizi e forniture.	Server di rete e armadio	Personal Computer manualmente	Intranet

Data di aggiornamento: 15/03/2010



segue

Tavola 5. Elenco dei trattamenti: cessioni a terzi di dati

Progressivo	Struttura	Ente verso il quale avviene il trasferimento dei dati	Tipologia di trasmissione
1.	AREA CONTROLLO DI GESTIONE E TRIBUTI U.O. Tributi – Riscossione coattiva entrate comunali	Un INCARICO esterno limitatamente alle posizioni ICI di fabbricati di gruppo D; A/4 e A/5 nonché A/10; la ditta incaricata entra in possesso di dati catastali degli immobili di proprietà dei contribuenti, delle copie di pratiche edilizie e della banca dati TARSU per la verifica della destinazione d'uso effettiva dell'immobile	Cartacea, elettronica
2.	AREA CONTROLLO DI GESTIONE E TRIBUTI U.O. Tributi – Riscossione coattiva entrate comunali	Equitalia Servizi: l'ufficio tributi spedisce al CNC annualmente copia delle denunce ai fini I.C.I. presentate dai contribuenti al Comune nell' anno precedente. Le denunce contengono l'anagrafica dei possessori d'immobili, gli estremi catastali, il periodo di possesso degli stessi. Inoltre, l'ufficio tributi spedisce ad equitalia servizi annualmente o secondo necessità gli elenchi dei contribuenti T.A.R.S.U. che hanno fatto richieste di sgravio e/o discarico totale e/o parziale di somme iscritte a ruolo coattivo e non dovute. Gli elenchi contengono l'anagrafica del contribuente facente richiesta, gli importi iscritti a ruolo e le somme discaricate e/o sgravate, e gli elenchi dei contribuenti morosi (sia per i tributi locali sia per entrate patrimoniali dell'ente) per l'estrazione del ruolo coattivo	Cartacea, elettronica
3.	Area Bilancio: servizio ragioneria e bilancio	I trattamenti di comunicazione di dati personale sono relativi alla trasmissione di copie di fatture passive/attive e dati economici necessari alla compilazione di dichiarazione IRAP, Mod. 770. Tali dati vengono inviati ad uno studio esterno, consulente in materia fiscale.	Cartacea, elettronica
4.	Area Bilancio: servizio Provveditorato Economato	Per svolgere i trattamenti indicati, il servizio si avvale dei servizi di un broker assicurativo, che riceve le denunce di sinistro sulle polizze assicurative comunali e le inoltra alle varie Compagnie Assicurative seguendo l'iter della pratica fino all'eventuale liquidazione del danno.	Cartacea, elettronica



segue

Progressivo	Struttura	Ente verso il quale avviene il trasferimento dei dati	Tipologia di trasmissione
5.	Area Servizi alla Persona e Comunicazione: Servizi Sociali, Politiche abitative, Sanità	Rispetto all'anagrafica utenti per bollettazione (orti, Centro Accoglienza Extracomunitari), i dati raccolti si riferiscono a nome, cognome, C.F., nazionalità, data e luogo di nascita, indirizzo, recapito telefonico, situazione economica; in caso di necessità di assistenza tecnico-informatica, vengono trasmessi alla ditta esterna fornitrice dei programmi (Ditta Softech di Bologna)	Elettronica
6.	Area Servizi alla Persona e Comunicazione: Servizi Sociali, Politiche abitative, Sanità	Rispetto alla gestione utenti SAD e per accesso rete servizi socio-sanitari integrati (interventi per anziani non-autosufficienti di cui alla L.R.5/94) i dati raccolti riguardano oltre all'anagrafica e recapito telefonico dell'utente, medico di medicina generale, dati anagrafici, posizione lavorativa e recapito telefonico dei parenti conviventi e non, condizioni socio-sanitarie e abitative dell'utente, nonché il progetto assistenziale individuale, ovvero gli interventi richiesti, usufruiti e proposti. Tali dati contenuti nella scheda relativa alla domanda e nella scheda di valutazione sociale vengono raccolti dall'ufficio e successivamente trasmessi, tramite il programma GARSIA, all'Azienda U.S.L., per la certificazione della non autosufficienza a cura della Commissione di Valutazione e di conseguenza per l'assegnazione del servizio appropriato al bisogno rilevato. L'utilizzo di GARSIA e la relativa trasmissione dei dati all'Azienda U.S.L. è prevista dall'Accordo di Programma per l'organizzazione e gestione della rete dei servizi rivolti alla popolazione anziana" (approvato con deliberazione di Consiglio Comunale n.85 del 22.09.2000). Anche questi dati, in caso di necessità di assistenza tecnico-informatica, vengono trasmessi alla ditta esterna fornitrice dei programmi (Ditta Softech di Bologna)	Elettronica
7.	Area Servizi alla Persona e Comunicazione: Servizi Sociali, Politiche abitative, Sanità	Rispetto alla gestione utenti contributo regionale a sostegno dell'affitto, è obbligo del Comune rendicontare alla Regione, entro i termini previsti dalla direttiva regionale, l'elenco dei beneficiari, che contiene dati anagrafici (nome, cognome, C.F., indirizzo) e l'importo del contributo liquidato.	Elettronica



segue

Progressivo	Struttura	Ente verso il quale avviene il trasferimento dei dati	Tipologia di trasmissione
8.	Area Servizi alla Persona e Comunicazione: Servizi Sociali, Politiche abitative, Sanità	Rispetto all'assegnazione alloggi E.R.P., la graduatoria definitiva, contenente i nominativi degli ammessi ed il punteggio a loro attribuito, viene trasmessa alla Regione Emilia Romagna per la pubblicazione sul BUR, così come previsto nel Regolamento Edilizia Residenziale Pubblica (approvato dal Consiglio Comunale con deliberazioni n°64 del 19.07.2002 e n°45 del 27.04.2004). Relativamente alle singole assegnazioni di alloggio E.R.P., il Comune trasmette all'ACER dati anagrafici e recapito telefonico di tutti i componenti del nucleo familiare dell'assegnatario, la certificazione di non titolarità di diritti reali per ciascun componente, oltre alla situazione economica del nucleo (calcolata ai sensi D.Lgs n. 109/98 e successive modificazioni ed integrazioni).	Cartacea, elettronica
9.	Area Servizi alla Persona e Comunicazione: Servizi Sociali, Politiche abitative, Sanità	Rispetto ai benefici economici previsti dalla L.448/98 (assegno per nucleo numeroso e per maternità) i dati si riferiscono all'anagrafica del richiedente e dei componenti il nucleo, la situazione economica del nucleo (calcolata ai sensi D.Lgs n. 109/98 e successive modificazioni ed integrazioni) e le modalità di pagamento del relativo beneficio. I dati vengono trasmessi all'I.N.P.S. per la liquidazione del contributo economico.	Elettronica
10.	Area Servizi alla Persona e Comunicazione: Servizi Sociali, Politiche abitative, Sanità	Rispetto alle invalidità civili, i dati riguardano l'anagrafica del richiedente ed eventuale coniuge, in caso di decesso dell'invalido, anagrafica degli eredi (se è presente il coniuge, anche data di matrimonio), data e luogo del decesso, del tutore (in caso di minori o interdetti), titolarità di pensioni o altri tipi di indennità, situazione lavorativa, eventuale ricovero in struttura con indicazione della denominazione ed indirizzo della struttura, eventuale iscrizione alle liste speciali del collocamento, eventuale frequenza scolastica o di centro riabilitativo (nel caso di minori), redditi dell'invalido ed eventuale coniuge. Tali dati vengono trasmessi al Comune di Bologna, Ufficio Invalidi Civili, così come previsto dalla vigente convenzione (approvata con deliberazione di Consiglio Comunale n°44 del 27.04.2004).	Cartacea

Progressivo	Struttura	Ente verso il quale avviene il trasferimento dei dati	Tipologia di trasmissione
11.	Area Servizi alla Persona e Comunicazione: Servizi Sociali, Politiche abitative, Sanità, Servizi educativi e scolastici	Rispetto alle Certificazioni ISEE, i dati si riferiscono all'anagrafica del richiedente e familiari, alle condizioni economiche, alla situazione di eventuale disabilità (ai sensi D.Lgs n. 109/98 e successive modificazioni ed integrazioni); tali dati vengono inseriti direttamente nel programma INPS (soggetto pubblico) al fine del rilascio dell'attestazione indicatore situazione economica del nucleo familiare (Dlgs. 109/1998 e 130/2000) e del conseguente eventuale beneficio, economico o di accesso ai servizi in cui tale requisito è previsto, per il richiedente.	Elettronica
12.	Area Servizi alla Persona e Comunicazione: Servizi Educativi Scolastici ,Sport: servizio nido	Trasferimento dati nuovi ammessi entro giugno di ogni anno alla Ditta esterna - attualmente Società Dolce di Bologna - che gestisce in appalto per il periodo 25.08.2008-31.07.2013 i servizi educativi per la prima infanzia Piccolo Giallo e Centro Giochi L'Oblò (determinazione . Area Servizi alla Persona n. 379 del 14.07.08)	Cartacea, elettronica
13.	Area Servizi alla Persona e Comunicazione: Servizi Educativi Scolastici ,Sport: servizio nido	Trasferimento dati anagrafici iscritti agli asili nido e trasmissione schede di anamnesi (dati sensibili) consegnate all'Ufficio Servizi Educativi e Scolastici dalle famiglie alla Azienda USL Bologna per monitoraggio sanitario relativo ai bambini che frequentano i nidi	Cartacea, elettronica
14.	Area Servizi alla Persona e Comunicazione: Servizi Educativi Scolastici ,Sport: centri estivi	Trasferimento dati iscritti entro maggio di ogni anno (e successivamente al bisogno) all'Istituzione SISTeR, organismo strumentale del Comune, costituito dall'1.09.2006, di cui fa parte personale comunale, al fine di consentire l'organizzazione del servizio; successivamente l'Istituzione trasferisce i dati degli iscritti alla Ditta esterna – attualmente Cooperativa Sociale Società Dolce di Bologna - che gestisce in appalto il servizio centri estivi comunali (determina Responsabile Area Servizi alla Persona n. 389 del 13.07.2009 aggiudicazione servizi integrazione scolastica parascolastici e centri estivi periodo settembre2009-settembre2013)	Cartacea, elettronica



segue

Progressivo	Struttura	Ente verso il quale avviene il trasferimento dei dati	Tipologia di trasmissione
15.	Area Servizi alla Persona e Comunicazione: Servizi Educativi Scolastici ,Sport: centri estivi	(refezione, pre post scuola, custodia, trasporto) trasferimento dati iscritti entro giugno di ogni anno all'Istituzione SISTeR (e successivamente al bisogno) al fine di consentire l'organizzazione dei servizi di refezione, pre post scuola, custodia, accompagnamento bus; successivamente l'Istituzione trasferisce i dati degli iscritti alla Ditta esterna – attualmente Cooperativa Sociale Società Dolce - che gestisce in appalto i servizi di accompagnamento bus e servizi pre post scuola e custodia comunali (determina Responsabile Area Servizi alla Persona n. 389 del 13.07.2009 aggiudicazione servizi integrazione scolastica parascolastici e centri estivi periodo settembre2009-settembre2013); l'Istituzione trasferisce inoltre i dati relativi agli iscritti al servizio di trasporto scolastico alla Ditta COSEPURI di Bologna – aggiudicataria del servizio di trasporto scolastico per il periodo gennaio 2008-settembre 2010 determinazione Direttore Istituzione SISTER n. 32 del 21.12.2007.	Cartacea, elettronica
16.	Area Servizi alla Persona e Comunicazione: Servizi Educativi Scolastici ,Sport: servizi scolastici	I dati anagrafici degli iscritti ai diversi servizi possono essere anche trasferiti, al bisogno, alla ditta esterna – Ditta Softech di Bologna - alla quale è stata affidata la fornitura del software per la gestione della bollettazione servizi scolastici, del nido e impianti sportivi (SOSIA), nonché il software per la formazione delle graduatorie degli asili nido (Gradus) e il software per l'accoglimento delle domande dei servizi scolastici (Sportello). Il trasferimento si potrà verificare in caso di problematiche legate al software e/o necessità di modifica dello stesso	Elettronica
17.	Area Servizi alla Persona e Comunicazione: Servizi Educativi – integrazione scolastica alunni portatori di handicap	Trasferimento dati iscritti entro agosto di ogni anno (e successivamente al bisogno) al fine di consentire l'organizzazione dell'integrazione scolastica alunni portatori di handicap, alla Ditta esterna – attualmente Cooperativa Sociale Società Dolce di Bologna - che gestisce in appalto tali servizi comunali (determina Responsabile Area Servizi alla Persona n. 389 del 13.07.2009 aggiudicazione servizi integrazione scolastica parascolastici e centri estivi periodo settembre2009-settembre2013)	Cartacea, elettronica

Progressivo	Struttura	Ente verso il quale avviene il trasferimento dei dati	Tipologia di trasmissione
18.	Area Servizi alla Persona: Servizi educativi e scolastici – recupero rette insolute	Trasferimento dati anagrafici utenti iscritti ai servizi refezione pre post scuola e trasporto negli anni scolastici passati alla Ditta AGERC di Cesenatico (FO) per svolgimento servizio recupero crediti pregressi rette servizi scolastici (determinazione Responsabile U.O. Entrate n. 380 del 26/6/07 e successive modifiche)	Cartacea, elettronica
19.	Area Servizi alla Persona e Comunicazione: Servizi Sociali, Politiche abitative, Sanità	Trasferimento dati anagrafici e sensibili relativi a soggetti, anche disabili, seguiti dal Servizio Sociale comunale ai fini della loro partecipazione alle vacanze per ragazzi e per disabili all'Ufficio di Piano del Distretto Pianura Est con sede presso il Comune di San Pietro in Casale	Cartacea, elettronica
20.	Area Servizi alla Persona e Comunicazione: Servizi Sociali, Politiche abitative, Sanità	Trasferimento all'Ufficio di Piano del Distretto Pianura Est con sede presso il Comune di San Pietro in Casale di dati anagrafici e sensibili relativi ai richiedenti contributi regionali per disabili gravi, previsti dalla L.R. 29/97 agli artt. 9 e 10	Cartacea, elettronica
21.	Area Servizi alla Persona e Comunicazione: Servizi Culturali, Politiche giovanili	I dati relativi all'anagrafica dei lettori Biblioteca vengono raccolti, gestiti e inseriti in locale e quindi inviati automaticamente al CIB (Centro inter-Bibliotecario dell'Università di Bologna) da cui si gestiscono le statistiche e i controlli (sui titoli). I dati personali comprendono nome, cognome, indirizzo e telefono, data di nascita, professione, titolo di studio, documento identità	Elettronica
22.	ISTITUZIONE SISTER Servizio Integrato scuola trasporto e refezione (costituita dall'1.09.2006), organismo strumentale del Comune preposto alla gestione dei servizi suddetti: centri estivi	Acquisizione dati iscritti al servizio centri estivi dal Comune (presentazione domande tramite URP entro metà maggio), con l'indicazione da parte dell'Ufficio Servizi educativi dei ragazzi certificati che necessitano di sostegno educativo aggiuntivo, al fine di organizzare e gestire il servizio; successivamente l'Istituzione trasferisce i dati degli iscritti ivi compresi dati relativi a ragazzi certificati iscritti al fine del supporto educativo alla Ditta esterna – attualmente Cooperativa Sociale Società Dolce di Bologna - che gestisce in appalto il servizio centri estivi comunali (Contratto Rep. 8832/2009) Si precisa che Società Dolce acquisisce già nel corso dell'anno scolastico i dati relativi a ragazzi certificati ai sensi della L. 104/92 (i medesimi che possono iscriversi anche ai centri estivi) in quanto aggiudicataria anche del servizio di integrazione scolastica alunni portatori di handicap.	Cartacea, elettronica



segue

Progressivo	Struttura	Ente verso il quale avviene il trasferimento dei dati	Tipologia di trasmissione
23.	ISTITUZIONE SISTER Servizio Integrato scuola trasporto e refezione: servizi parascolastici (pre post scuola custodia) e accompagnamento bus	Acquisizione dati iscritti ai servizi pre post scuola e al trasporto scolastico dal Comune (presentazione domande tramite URP), al fine di organizzare e gestire i servizi; successivamente l'Istituzione trasferisce i dati degli iscritti alla Ditta esterna – attualmente Cooperativa Sociale Società Dolce di Bologna - Consorzio Epta che gestisce in appalto i servizi parascolastici e accompagnamento bus (Contratto Rep. 8832/2009)	Cartacea, elettronica
24.	ISTITUZIONE SISTER Servizio Integrato scuola trasporto e refezione: trasporto scolastico	Acquisizione dati iscritti al servizio di trasporto scolastico dal Comune (presentazione domande tramite URP), al fine di organizzare e gestire il servizio; successivamente l'Istituzione trasferisce i dati degli iscritti alla Ditta esterna – COSEPURI di Bologna - che gestisce in appalto il servizio di trasporto scolastico (determinazione Direttore Istituzione SISTER n. 32 del 21.12.2007)	Cartacea, elettronica
25.	Area Tecnica: U.O. Commercio/Servizi Amministrativi	CCIAA : Richieste verifiche dati autorizzazioni commerciali - saltuario	Cartacea, elettronica
26.	Area Tecnica: U.O. Commercio/Servizi Amministrativi	Questura di Bologna Comando Carabinieri di Castenaso: Dati anagrafici dei richiedenti l'effettuazione di manifestazioni varie (spettacoli viaggiatori, fiere, sagre, fuochi d'artificio)	Cartacea
27.	Area Tecnica: U.O. Commercio/Servizi Amministrativi	USL: dati anagrafici dei richiedenti il rilascio di patenti per l'utilizzo di gas tossici	Cartacea
28.	Area Tecnica: U.O. Commercio/Servizi Amministrativi	Questura di Bologna: dati anagrafici dei richiedenti l'autorizzazione alla vendita di cose usate e antiche	Cartacea
29.	Area Tecnica: U.O. Lavori pubblici	Osservatorio Lavori Pubblici: dati anagrafici su ditte aggiudicatrici o loro comportamenti - cadenza saltuaria/annuale	Cartacea, elettronica
30.	Area Tecnica: U.O. Edilizia Patrimonio Sportello unico	Arpa- USL, altri enti: dati anagrafici pratiche edilizie e Sportello unico imprese – cadenza correlata alla presentazione pratiche	Cartacea
31.	Area Tecnica: U.O. Edilizia Patrimonio sportello unico e U.O. Commercio/Servizi Amministrativi	Agenzia delle Entrate Ministero delle finanze: anagrafe tributaria – cadenza annuale	Elettronica
32.	Area Tecnica: U.O. Edilizia Patrimonio sportello unico	Società ICA di La Spezia, Provincia di Bologna: dati anagrafici titolari di autorizzazioni installazione cartelli/insegne	Cartacea, elettronica
33.	Area Tecnica: U.O. Servizi Ambientali	Centro Agricoltura Ambiente di Crevalcore (direzione tecnica del U.O. di disinfezione- assistenza tecnica-scientifica) dati anagrafici di cittadini che utilizzano prodotti larvicidi	Cartacea, elettronica

Progressivo	Struttura	Ente verso il quale avviene il trasferimento dei dati	Tipologia di trasmissione
34.	Area Tecnica: U.O. Servizi Ambientali	Regione Emilia Romagna : dati anagrafici richiedenti il contributo per la trasformazione di impianti auto da benzina a gpl/metano	elettronica
35.	Area Tecnica: U.O. Servizi Ambientali	Hera Bologna : copia autorizzazioni allo scarico produttive	Cartacea
36.	Polizia Municipale: Servizio di Polizia Municipale	L'attività di rimozione e custodia veicoli é affidata alla Ditta DEPOSITERIA GIAN PAOLO SNC. DI SCHIAVINA GIAN PAOLO, con Sede In Castenaso Via Del Frullo 32, che svolge i compiti con proprio personale dipendente	Cartacea
37.	Polizia Municipale: Servizio di Polizia Municipale	L'attività di CONFERIMENTO E CUSTODIA GATTI RANDAGI é affidata all'Associazione "CANILE INTERCOMUNALE Comuni di Budrio, Castenaso, Medicina e Molinella, Rifugio di Bagnarola – ONLUS", con sede in Budrio (BO) Via Fondazza n.7/A, gestita da volontari che svolge i compiti con proprio personale	Cartacea
38.	Polizia Municipale: Servizio di Polizia Municipale	Infortunistica stradale documentazione relativa ai rilievi di sinistri stradali. Rilascio ad aventi diritto.	Cartacea
39.	Polizia Municipale: Servizio di Polizia Municipale	Servizio di recupero crediti relativo ai provvedimenti sanzionatori non corrisposti nei termini e affidata alla ditta EQUITALIA POLIS S.P.A. , via del Lavoro 47, Casalecchio di Reno (BO)	Cartacea Elettronica
40.	Area Affari generali - Servizio URP	Accesso a documenti amministrativi: ricevimento istanza al protocollo e trasmissione a ufficio responsabile del procedimento. Se l'istanza riguarda procedimenti dell'area: verifica diritto d'accesso e consegna/visione del documento	Cartacea, elettronica



segue

Progressivo	Struttura	Ente verso il quale avviene il trasferimento dei dati	Tipologia di trasmissione
41.	Area Affari generali: Stato civile – anagrafe-liste elettorali:	Ricevimento denunce e redazione atti – trasmissione comunicazione al comune competente e ad altri soggetti previsti dalla legge (es. denunce di morte all'INPS) Trascrizione atti provenienti da altri enti – Ricevimento istanze di iscrizione variazione anagrafica Richiesta accertamento al Corpo P.M. per iscrizione anagrafica – Cancellazione anagrafiche – Rilascio certificati – Elenchi ai soggetti aventi diritto per legge (pubbliche amministrazioni per attività istituzionali) – Se trattasi di stranieri, controllo permessi di soggiorno – Liste elettorali – Predisposizione e revisione liste elettorali – Rilascio liste elettorali nei casi previste dalla Legge: Diritti politici elettorato attivo e passivo – Albi dei Presidenti e scrutatori – Autentica firme di sottoscrittori e candidati, ricevimento liste comunali – Rilascio tessere elettorali, consegnate agli interessi tramite messo comunale – Predisposizione ed aggiornamento albo Giudici Popolari	Cartacea, elettronica
42.	Area Affari generali: Stato civile – anagrafe-liste elettorali:	Trasmissione dati INASIA invio dati anagrafici per l'aggiornamento banca dati istituita presso il ministero	Elettronica
43.	Area Affari generali: Stato civile – anagrafe-liste elettorali:	Invio elenchi ogni mese Usl Pediatra Ufficio Registro carabinieri Questura Registro tumori	Cartacea
44.	Area Affari generali: Stato civile – anagrafe-liste elettorali:	Trimestrale :Ufficio Entrate Casellario Giudiziale	Cartacea
45.	Area Affari generali: Stato civile – anagrafe-liste elettorali:	Invio elenchi deceduti Direzione Provinciale tesoro INPDEL	Cartacea
46.	Area Affari generali: Stato civile – anagrafe-liste elettorali:	Ricevimento istanze e rilascio relativa autorizzazione di trasporto salme, cremazione , affido e dispersione ceneri	Cartacea
47.	Area Affari generali: Stato civile – anagrafe-liste elettorali:	Rilascio attestazioni per cittadini comunitario a seguito di documentazione presentata	Cartacea
48.	Area Affari generali: Servizio Segreteria	Documentazione attività istituzionale di organi politici	Cartacea, elettronica
49.	Area Affari generali: Servizio Segreteria	Pubblicazione all'albo di delibere e ordinanze	Cartacea, elettronica
50.	Area Affari generali: Servizio Segreteria e URP	Sito internet del Comune di Castenaso	Elettronico
51.	Area Affari generali: Servizio URP	Ricevimento denunce infortuni e cessione fabbricati (attività di PS)	Cartacea, elettronica
52.	Area Affari generali: Servizio URP	Rilascio contrassegni invalidi, previa verifica di certificazione medica per sussistenza requisiti	Cartacea, elettronica
53.	Area Affari generali: Servizio URP	Periodico Comunale, adempimenti burocratici, rapporti col direttore del periodico	Cartacea, elettronica
54.	Area Affari generali: Servizio Segreteria Sindaco	Benefici economici: Erogazione contributi ad enti e associazioni non a privati	Cartacea, elettronica

Progressivo	Struttura	Ente verso il quale avviene il trasferimento dei dati	Tipologia di trasmissione
55.	Segretario Generale : Sviluppo Organizzativo e Politiche del Personale	Dipendenti della Società alla quale viene conferito incarico annuale per pratiche previdenziali: accesso e acquisizione fascicoli dei dipendenti	Cartacea, elettronica
56.	Segretario Generale : Sviluppo Organizzativo e Politiche del Personale	Medico competente che esegue i controlli sanitari ai sensi del D.Lgs.81/2008 e utilizza i dati nel pieno rispetto della normativa sulla privacy	Cartacea, elettronica
57.	Segretario Generale : Sviluppo Organizzativo e Politiche del Personale	Dipendenti della Ditta esterna fornitrice del software gestionale abilitata ad accedere ai dati del trattamento personali, giuridici ed economici del personale dipendente.	Cartacea, elettronica
58.	Segretario Generale : Sviluppo Organizzativo e Politiche del Personale	Dipendenti della ditta esterna fornitrice del software del programma di gestione presenze/assenze	Cartacea, elettronica

Data di aggiornamento: 15/03/2010

Note settore Area Affari Generali

I trattamenti svolti rientrano nelle seguenti tipologie:

- Accesso a documenti amministrativi: ricevimento istanza al protocollo e trasmissione a ufficio responsabile del procedimento. Se l'istanza riguarda procedimenti dell'area: verifica diritto d'accesso e consegna/visione del documento;
- Stato civile -anagrafe -liste elettorali :
 - o Ricevimento denunce e redazione atti- trasmissione comunicazione al comune competente e ad altri soggetti previsti dalla legge (es. denunce di morte all'INPS);
 - o Trascrizione atti provenienti da altri enti ;
 - o Ricevimento istanze di iscrizione/variazione anagrafica;
 - o Richiesta accertamento al Corpo P.M. per iscrizione anagrafica;
 - o Cancellazioni anagrafiche;
 - o Rilascio certificati;
 - o Elenchi ai soggetti aventi diritto per legge (pubbliche amministrazioni per attività istituzionali);
 - o Se trattasi di stranieri, controllo permessi di soggiorno;
 - o Liste elettorali;
 - o Predisposizione e revisioni liste elettorali;
 - o Rilascio liste elettorali nei casi previsti dalla legge : Diritti politici elettorato attivo e passivo;
 - o Albi dei Presidenti e scrutatori;
 - o Autentica firme di sottoscrittori e candidati, ricevimento liste comunali;
 - o Rilascio tessere elettorali, consegnate agli interessati tramite messo comunale;



segue

- o Predisposizione ed aggiornamento albo Giudici popolari.
- Documentazione attività istituzionale di organi politici
- Pubblicazione all'albo di delibere, ordinanze, determinazioni
- Sito internet del Comune di Castenaso
- Periodico comunale, adempimenti burocratici, rapporti col direttore del periodico
- Benefici economici : Erogazione contributi ad enti e associazioni, non a privati
- Altre materie :
 - o Comunicazione al Ministero delle Finanze dei secondi nati o ulteriori o adottati ;
 - o Ricevimento denunce infortuni.(attività di PS);
 - o Rilascio contrassegni invalidi, previa verifica certificazione medica per sussistenza requisiti.

Note settore Corpo di Polizia Municipale: Servizio di Polizia Municipale

Le attività svolte comprendono :

- Contravvenzioni CDS
- Contravvenzioni Regolamenti comunali, Leggi regionali e statali
- Attività relativa all'infortunistica stradale
- Attività relativa agli infortuni sul lavoro
- Attività di polizia annonaria, commerciale e amministrativa
- Attività di vigilanza edilizia, ambientale, sanitaria, urbana e rurale
- Attività di rilascio autorizzazioni invalidi
- Attività di informazione e accertamento
- Attività amministrativa per rilascio autorizzazioni TOSAP, pubblicità temporanea.
- Attività di Pubblica Sicurezza
- Attività di Educazione stradale scolastica

Note servizio Controllo di Gestione all'interno dell'Area Controllo di Gestione

Si tratta di un servizio di recente istituzione, che attualmente non svolge alcun trattamento di dati personali.

Il censimento dei beni che rientrano nel piano di sicurezza

In questa sezione del documento censiamo tutti gli strumenti informatici che hanno una qualche interferenza con il piano di sicurezza dell'ente e che contengono delle banche dati. In primo luogo presentiamo l'elenco delle sedi interessate dal progetto.

Tavola 6.riepilogo delle sedi dell'ente

Progressivo	Denominazione sede	Tipo di collegamento
1.	Palazzo Comunale	Centro stella
2.	Ufficio Tecnico	LAN in fibra ottica
3.	Polizia Municipale	LAN in fibra ottica
4.	Casa Bondi/Biblioteca	LAN in fibra ottica
5.	Magazzini comunali	MPLS
6.	Cimitero comunale	MPLS
7.	Cucina centrale	MPLS
8.	Centro culturale La Scuola Marano	nessuno
9.	Asilo nido Piccolo giallo	MPLS
10.	Asilo nido Piccolo blu	MPLS
11.	MUV Museo Villanoviano	MPLS
Data di aggiornamento: 15/03/2010		

Di seguito presentiamo l'elenco dei beni informatici che sono atti a contenere banche dati o a permetterne in un qualunque modo l'utilizzo.

Tavola 7. Riepilogo del censimento dei beni informatici che rientrano nel piano di sicurezza dell'ente

Servizi funzionali										
Device	File server	Altri server	DB Server gestionale	E-mail	Apps gestionali	Servizi di gestione	Router o switch	Marca	S.O	F.T.
Municipio										
SERVER01				X				Vmware	Windows NT 4.0 Sp6a	
SERVER02		X			X	Printer Server,		Assemblato Vmware Server	Windows 2000 server SP4	
SERVER10	X				X			HP ProLiant DL380 G3	Windows 2000 server SP4	Raid 5
SERVER15		X			X	Terminal Server,		Fujitsu Siemens Primergy	Windows 2000 server SP4	Raid 5
SERVER16			X					Fujitsu Siemens Primergy	Windows 2003 Server SP1	Raid 5
MAMMUT		X				X		Assemblato	Linux Debian	Raid 5
BISONTE		X				X		HP	Linux Debian	Raid 5
SVRCASTENASO		X				Vmware Server		HP ProLiant DL380 G3	Windows 2000 server SP4	Raid 5
ADCAST02						AD Controller, DNS, DHCP		VMware	Windows 2000 server SP4	
ADCAST04						AD Controller, DNS, DHCP		VMware	Windows 2000 server SP4	
BCKSERVER						Veritas Server		IBM Netfinity 3000	Windows 2000 Professional SP4	Raid 1
HELPDESK		X	X					Vmware	Linux Ubuntu Server 6.06	
LDAPBIBLIO		X				OpenLDAP		Vmware	Linux Ubuntu Server 7.10	
ADCAST02						AD Controller, DNS		Vmware	Windows 2000 server SP4	
MAILCLEANER		X						Vmware	Linux Debian	
OCIPETE		X						Vmware	Linux Debian	
SERVERWUS		X						Vmware	Windows 2003 Server SP1	

Servizi funzionali										
Device	File server	Altri server	DB Server gestionale	E-mail	Apps gestionali	Servizi di gestione	Router o switch	Marca	S.O	F.T.
WEBSRVCITYTOWN	X	X						Vmware	Windows 2000 server SP4	
CASTCEICNSD		X						Vmware	Windows 2000 Professional SP4	
Virtuoso01		X				X		Assemblato	VMware ESXi 3.5	
Virtuoso02		X				X		Assemblato	VMware ESXi 3.5	
EleOnLine		X EleOnLine Web						Vmware	Debian Linux	
CastBackupSRV		X				SyncToy Microsoft		Vmware	Windows XP SP3	
MulteWeb		X				X Tomcat		Vmware	Linux Debian 5	
CAST0817	X							Lacie	NAS	
CAST0818	X							Lacie	NAS	
Switch 1 Armadio CED							X	Allied Telesyn	n.a.	Nessuno
Switch 2 Armadio CED							X	Allied Telesyn	n.a.	Nessuno
Switch 3 Armadio CED							X	3Com	n.a.	Nessuno
Switch Armadio Server							X	HP procurve	n.a.	Nessuno
Ufficio tecnico										
Switch vari							X	Vari	n.a.	Nessuno
Polizia Municipale										
Switch vari							X	Vari	n.a.	Nessuno
Servizi Sociali										
Switch vari							X	Vari	n.a.	Nessuno
Biblioteca										
Switch vari							X	Vari	n.a.	Nessuno
Data di aggiornamento: 15/03/2010										

Analisi organizzativa dell'ente

Scopo di questa fase è capire l'impatto che la sicurezza ha determinato nella definizione dell'organigramma dell'ente, se di impatto si può parlare.

Si tratta di partire dall'organigramma dell'ente per capire quali sono i centri di decisione che hanno influito o potranno influire sulle decisioni in merito alla sicurezza. Per le aziende certificate ISO questo processo è già stato largamente affrontato e documentato; nonostante questo rimane la necessità di controllare detto processo e di valutarne l'aggiornamento.

A titolo esemplificativo dell'impatto che una non accurata analisi organizzativa e giuridica dello stato dell'organizzazione può avere, presentiamo un esempio emblematico circa i rischi che corre l'ente dando il problema della sicurezza, "per scontato".

Il problema riguarda la teoria della downstream liability, un tema scottante in cause civili per fenomeni di hacking. Il problema sorge quando una organizzazione colpita non potrà essere risarcita nei danni subiti da un hacker (che spenderà tutti i suoi soldi per un legale). La moderna giurisprudenza afferma che l'organizzazione lesa potrà rivalersi "a valle" nei confronti dell'organizzazione che ha permesso all'hacker di entrare nei suoi sistemi consentendogli l'attacco!!

L'organizzazione chiamata in causa dovrà dimostrare di non essere stata negligente, di disporre di misure di sicurezza aggiornate ed adeguate.

Questa analisi ha, quindi, lo scopo di analizzare l'organizzazione del Comune di Castenaso per fare in modo che essa non possa essere trovata "negligente".

Presentiamo in primo luogo l'organigramma dell'ente, evidenziando in colore giallo i centri di decisione in merito alla sicurezza dei dati:

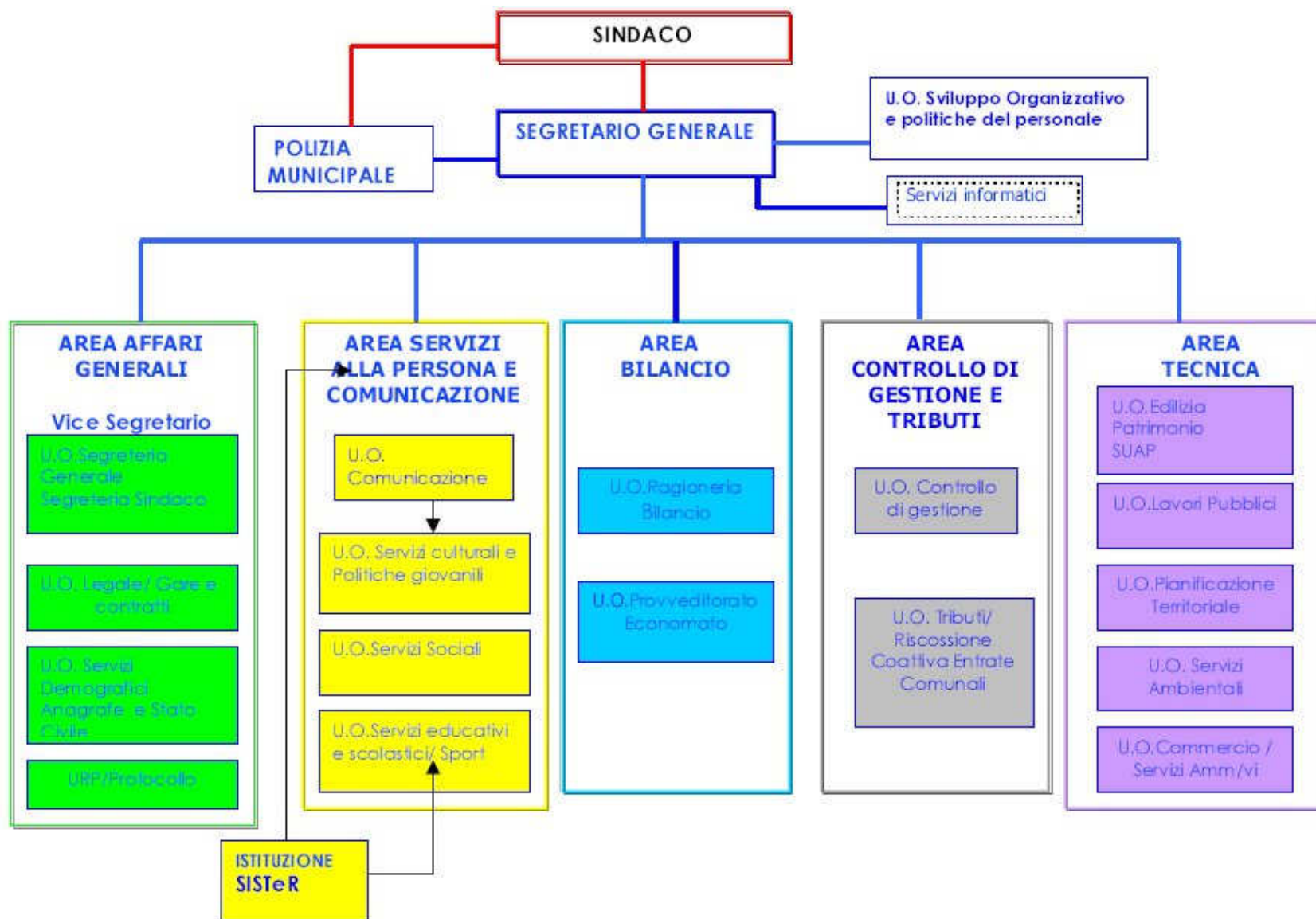


Figura 1 L'organigramma del Comune di Castenaso

Da una semplice lettura si può comprendere chi nell'organizzazione del Comune di Castenaso, con la sua attività e con le sue decisioni, può influire sulla sicurezza nella gestione dei dati. Tali persone sono state oggetto di percorsi di motivazione e di processi formativi, circa l'argomento.

Presentiamo a questo punto l'elenco degli incaricati, il gruppo di appartenenza ed il profilo ad essi associato.

Tavola 8.riepilogo degli incaricati

NOME E COGNOME	GRUPPO	SEDE	PROFILO
Dal Pozzo Daniela	U.O. Sviluppo Organizzativo e Politiche del Personale	Municipio	alto
Bergami Annalisa	U.O. Sviluppo Organizzativo e Politiche del Personale	Municipio	normale
Dall'Olio Antonella	U.O. Sviluppo Organizzativo e Politiche del Personale	Municipio	normale
Gabriele Mariangela	U.O. Sviluppo Organizzativo e Politiche del Personale	Municipio	normale
Capasso Francesco	Servizi Informatici	Municipio	alto
Tinti Simone	Servizio Informatico	Municipio	Alto
Bonino Vincenza	Area Tecnica	Ufficio tecnico via Gramsci 21	Normale
Rizzoli Angela	Area Tecnica	Ufficio tecnico via Gramsci 21	Normale
Sunzeri Giuseppina	Area Tecnica	Ufficio tecnico via Gramsci 21	Normale
Focaccia Claudia	Area Tecnica	Ufficio tecnico via Gramsci 21	Normale
Bergamini Chiara	Area Tecnica	Ufficio tecnico via Gramsci 21	Alto
Rimondini Serena	Area Tecnica	Ufficio tecnico via Gramsci 21	Alto



segue

Vannini Maurizio	Area Tecnica	Ufficio tecnico via Gramsci 21	Normale
Pazzini Marco	Area Tecnica	Ufficio tecnico via Gramsci 21	Normale
Ruscelloni Fabrizio	Area Tecnica	Ufficio tecnico via Gramsci 21	Alto
Matteuzzi Andrea	Area Tecnica	Ufficio tecnico via Gramsci 21	Alto
Altília Leonardo	Area Tecnica	Ufficio tecnico via Gramsci 21	Normale
Mazzanti Alberto	Area Tecnica	Ufficio tecnico via Gramsci 21	Normale
Carini Paolo	Area Tecnica	Ufficio tecnico via Gramsci 21	Alto
Nicodemo Claudia	Area Tecnica	Ufficio tecnico via Gramsci 21	Alto
Fratti Simonetta P.I. 02472271200	Area Tecnica	Ufficio tecnico via Gramsci 21	Normale
Zita Piergiorgio	Area Tecnica	Ufficio tecnico via Gramsci 21	Normale
BAGLIONI GIOVANNI	P.M.	Via Nasica 9-11	Normale
BIGNAMI CRISTINA	P.M.	Via Nasica 9-11	Alto
BORTOLINI VILLIAM	P.M.	Via Nasica 9-11	Normale
BOSELLO MICHELE	P.M.	Via Nasica 9-11	Normale
CORTESE ALESSIO	P.M.	Via Nasica 9-11	Normale
DISSETTE PAOLO	P.M.	Via Nasica 9-11	Normale



segue

FABBRI STEFANO	P.M.	Via Nasica 9-11	Alto
FRANCHINI PATRIZIA	P.M.	Via Nasica 9-11	Normale
FUNICELLI MIRKO	P.M.	Via Nasica 9-11	Normale
MELILLO ATTILIO	P.M.	Via Nasica 9-11	Normale
SPERA GIANNI	P.M.	Via Nasica 9-11	Normale
VENTURI SIMONA	P.M.	Via Nasica 9-11	Normale
ZINI RAFFAELLA	P.M.	Via Nasica 9-11	Normale
MARINA GOTTI	AREA SERVIZI PERSONA E COMUNICAZIONE	CASA BONDI	ALTO
MONICA TARTARINI	AREA SERVIZI PERSONA E COMUNICAZIONE	CASA BONDI	NORMALE
RITA RIMONDINI	AREA SERVIZI PERSONA E COMUNICAZIONE	CASA BONDI/BIBLIOTECA	ALTO
TONDINI ROBERTA	AREA SERVIZI PERSONA E COMUNICAZIONE	CASA BONDI	NORMALE
ANNA GIORDANO	AREA SERVIZI PERSONA E COMUNICAZIONE	CASA BONDI	NORMALE
MONIA ZINI	AREA SERVIZI PERSONA E COMUNICAZIONE	CASA BONDI	NORMALE
ANNA BAIA	AREA SERVIZI PERSONA E COMUNICAZIONE	CASA BONDI	NORMALE
ALICE D'AURIA	AREA SERVIZI PERSONA E COMUNICAZIONE	CASA BONDI	NORMALE
LUANA ANDRAGHETTI	AREA SERVIZI PERSONA E COMUNICAZIONE	CASA BONDI	NORMALE
ELENA FLAMINI	AREA SERVIZI PERSONA E COMUNICAZIONE	CASA BONDI	NORMALE
MARMIR MIRANDA	AREA SERVIZI PERSONA E COMUNICAZIONE	BIBLIOTECA	NORMALE
ORSONI LETIZIA	AREA SERVIZI PERSONA E COMUNICAZIONE	BIBLIOTECA	NORMALE



segue

EMANUELA VITA	AREA SERVIZI PERSONA E COMUNICAZIONE Dipendente Coop. Macchine Celibi, concessionario del Centro Giovanile	CASA BONDI CENTRO GIOVANILE Centro Culturale LA SCUOLA	NORMALE
SINDACO MARINA	AREA SERVIZI PERSONA E COMUNICAZIONE Dipendente Coop. Macchine Celibi, gestore del Museo Civiltà Villanoviana	CASA BONDI MUV	NORMALE
ELENA PAOLUCCI	AREA SERVIZI PERSONA E COMUNICAZIONE Dipendente Coop. Macchine Celibi, gestore del Centro Culturale LA SCUOLA	CASA BONDI Centro Culturale LA SCUOLA	NORMALE
CASU RAFFAELLA	ISTITUZIONE SISTER/AREA SERVIZI PERSONA E COMUNICAZIONE	CASA BONDI	ALTO
EMANUELA TUGNOLI	ISTITUZIONE SISTER	CASA BONDI	NORMALE
ELISA LUI	Area affari Generali	Sede Comunale P.zza Bassi n. 1	ALTO
NADIA SAPORI	URP/Segreteria	Sede Comunale- P.zza Bassi 1	ALTO
BUTTAZZI PAOLA	URP	“	NORMALE
AMORATI FLAVIA	URP	“	NORMALE
SPALLETTI ADRIANA	URP	“	NORMALE
COSTA MARINA	URP	“	NORMALE
FAVALE MARIA MATILDE	URP	“	NORMALE
VECCHI SIMONETTA	Segreteria	“	NORMALE

RANZOLIN LUCA	Contratti	“	NORMALE
LANDINI MIRIAM	Segreteria Sindaco	“	NORMALE
PASQUALI LUCA	Segreteria Generale	“	NORMALE
BARACANI ANTONELLA	Segreteria Generale		NORMALE
MACCAGNANI COSETTA	Servizi Demografici	“	ALTO
CAPPELLI ANNA MARIA	Servizi Demografici	“	NORMALE
STRADA CARLOTTA	Servizi Demografici	“	NORMALE
GALLI LUISA	Servizi Demografici	“	NORMALE
COSTA MARINA	Servizi Demografici	“	NORMALE
MASSIMILIANO TUNDO	AREA BILANCIO	P.ZZA BASSI, 1	ALTO
LUISELLA CIMINO	SERVIZIO BILANCIO	P.ZZA BASSI, 1	ALTO
ROBERTA BENEDETTI	SERVIZIO BILANCIO	P.ZZA BASSI, 1	NORMALE
ALESSANDRO GARZON	CONSULENTE ESTERNO	VIA SPINELLI, 6 – PORTO MANTOVANO (MN)	MINIMO
ITALO FERIOLI P.I. 00160141206	CONSULENTE ESTERNO	Via Stalingrado n.26 - Bologna	MINIMO
CLAUDIA MINARDI	U.O PROVVEDITORATO ECONOMATO	COMUNE	ALTO
CHIARA CLEMENTE	U.O PROVVEDITORATO ECONOMATO/U.O BILANCIO	COMUNE	NORMALE
ALESSIA BIANCHINI FINO DAL 19.10.2009 AL 30.09.2010	U.O PROVVEDITORATO ECONOMATO/U.O BILANCIO	COMUNE	NORMALE
BONORI MONICA	AREA CONTROLLO DI GESTIONE E TRIBUTI	CASA BONDI/PALAZZO	ALTO



segue

COMUNALE			
CIOMMI GIADA	CONTROLLO DI GESTIONE	PALAZZO COMUNALE	NORMALE
GIOSUE' ELETTRA	U.O TRIBUTI . RISCOSSIONE COATTIVA ENTRATE COMUNALI	PALAZZO COMUNALE	ALTO
BIANCHI DANIELA	U.O TRIBUTI . RISCOSSIONE COATTIVA ENTRATE COMUNALI	PALAZZO COMUNALE	NORMALE
DONATI DANIELA	U.O TRIBUTI . RISCOSSIONE COATTIVA ENTRATE COMUNALI	PALAZZO COMUNALE	NORMALE
GALLI ELISA	U.O TRIBUTI . RISCOSSIONE COATTIVA ENTRATE COMUNALI	PALAZZO COMUNALE	NORMALE
Data di aggiornamento 15/03/2010			



segue

Tavola 9.riepilogo dei profili

GRUPPO	PROFILO	CARATTERISTICHE DEL PROFILO
Tutti i gruppi	Normale	Sono consentite tutte e sole le operazioni di lettura e scrittura dei dati (quindi di modifica) per l'ordinario svolgimento della propria mansione
Tutti i gruppi	Minimo	Sono consentite tutte e sole le operazioni di lettura per l'ordinario svolgimento della propria mansione
Tutti i gruppi	Alto	Sono consentite tutte e sole le operazioni di lettura e scrittura (quindi di modifica) per l'ordinario svolgimento della propria mansione e la possibilità di modificare i diritti degli altri membri del gruppo

Rapporti con professionisti ed incaricati non dipendenti dell'ente

Allo scopo di assicurare il rispetto del codice sulla tutela dei dati personali, anche coloro che entrano in qualche modo in rapporto con l'ente senza diventarne dipendenti a tempo indeterminato, sono tenuti ad un comportamento corretto.

Per essere sicuri di ciò, il comune, nella sottoscrizione dell'incarico, ha aggiunto i seguenti punti:

- L'incaricato è autorizzato ad intervenire sui dati e sui sistemi informativi gestiti dal comune solo con atti strettamente necessari alla prestazione dei servizi oggetto di contratto, ed è fatto esplicito divieto di consultare, copiare, cancellare e fare qualunque operazione sui dati oggetto di trattamento, a meno di diversa autorizzazione scritta da parte del responsabile del trattamento dei dati.
- Il titolare si riserva di fare controlli sull'operato del responsabile esterno in qualunque momento e con qualunque mezzo consentito dalla legge.
- Il soggetto cui le attività sono affidate dichiara:
 - o di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, possono essere dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
 - o di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
 - o di adottare le istruzioni specifiche ricevute per il trattamento dei dati personali attraverso il manuale degli incaricati;
 - o di impegnarsi a relazionare ogni volta che è reputato necessario sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
 - o di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Le suddette dichiarazioni sono oggetto di specifica firma di accettazione da parte dell'incaricato.



segue

Distribuzione dei compiti e delle responsabilità (regola 19.2 dell'Allegato B al Codice)

In questa sezione è costruita una mappa che associa ad ogni struttura (o reparto, dipartimento, ufficio) i trattamenti da questa effettuati, descrivendo sinteticamente l'organizzazione della struttura medesima e le relative responsabilità. Ci si può riferire anche ad analoghe documentazioni già predisposte dal titolare (ordinamenti, ordini di servizio, regolamenti interni).

Tavola 10.distribuzione dei compiti e delle responsabilità

Struttura	Responsabile del trattamento	Servizio	Responsabile di settore/servizio P.O.	Trattamenti operati dalla struttura	Compiti della struttura
Segretario Generale	Dr. Andrea Fanti	Segretario generale	Dr. Andrea Fanti	143,144,145,146,147,148,149	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Affari Generali	Dr.ssa Elisa Lui	Segreteria del Sindaco	Dr. Andrea Fanti		
Direzione Generale	Dr. Andrea Fanti	Sviluppo Organizzativo e Politiche del Personale	Daniela Dal Pozzo	132, 133, 134,135,136,137,138,139,140 141,142	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Polizia Municipale	Stefano Fabbri	Polizia Municipale	Stefano Fabbri	119,120,121,122,123,124,125,126,127 128,129,130,131	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Affari Generali	Dr.ssa Elisa Lui	U.O. Segreteria Generale	Nadia Saponi	1,2,3,4,5,6,17,27,28,	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Affari Generali	Dr.ssa Elisa Lui	URP/Protocollo	Nadia Saponi	1,2,3,4,5,6,16,18,29	
Area Affari Generali	Dr.ssa Elisa Lui	Legale e contratti	Elisa Lui	19,20,21,22,23,24,25	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa

Struttura	Responsabile del trattamento	Servizio	Responsabile di settore/servizio P.O.	Trattamenti operati dalla struttura	Compiti della struttura
Area Affari Generali	Dr.ssa Elisa Lui	Servizi demografici	Cosetta Maccagnani	7,8,9,10,11,12,13,14,15	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Servizi alla Persona e Comunicazione	Marina Gotti	U.O. Comunicazione	Marina Gotti		Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Servizi alla Persona e Comunicazione	Marina Gotti	Servizi culturali e Politiche giovanili	Rimondini Rita		Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Servizi alla Persona e Comunicazione	Marina Gotti	U.O. Servizi Sociali	Tartarini Monica	41,42,43,44,45,46,47,48,49,50,51,66, 67,68,118	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Servizi alla Persona e Comunicazione	Marina Gotti	Servizi educativi e scolastici/ Sport	Casu Raffaella	52,53,54,55,56,57,60,64,65,69,70,71,72 73,74	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Istituzione SISTER	Marina Gotti	Istituzione SISTER	Casu Raffaella	58,,59,61,62,63	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa

Struttura	Responsabile del trattamento	Servizio	Responsabile di settore/servizio P.O.	Trattamenti operati dalla struttura	Compiti della struttura
Area Bilancio	Massimiliano Tundo	U.O. Ragioneria Bilancio	Massimiliano Tundo	34,35,40	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Bilancio	Massimiliano Tundo	U.O. Proveditorato Economato	Minardi Claudio	36,37,38,39	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Controllo di Gestione e Tributi	Bonori Monica	Controllo di Gestione	Bonori Monica		Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Controllo di Gestione e Tributi	Bonori Monica	Servizio Entrate	Giosuè Elettra	30,31,32,,33	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Tecnica	Ruscelloni Fabrizio	Edilizia Patrimonio SUAP	Ruscelloni Fabrizio	75,76,77,78,79,80,81,82,83,84,85,86,87	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Tecnica	Ruscelloni Fabrizio	Lavori Pubblici	Rimondini Serena	88,89,90,91,106,107	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Tecnica	Ruscelloni Fabrizio	Pianificazione Territoriale	Nicodemo Claudia	105,116,117	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa

Struttura	Responsabile del trattamento	Servizio	Responsabile di settore/servizio P.O.	Trattamenti operati dalla struttura	Compiti della struttura
Area Tecnica	Ruscelloni Fabrizio	Servizi Ambientali	Carini Paolo	98,99,100,101,102,103,104,112,113,114,115	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa
Area Tecnica	Ruscelloni Fabrizio	Commercio / Servizi Amm/vi	Bergamini Chiara	92,93,94,95,96,97,108,109,110,111	Acquisizione – caricamento e cancellazione dati – consultazione – comunicazione a terzi – stampa

Data di aggiornamento: 15/03/2010

L'accesso alle strutture fisiche dell'ente

Vogliamo ora mettere in evidenza chi ha le “chiavi” per poter accedere alle strutture dell'ente: lo facciamo con la seguente tabella riepilogativa. Ricordiamo che tutto lo stabile è protetto da chiave e sistema di allarme

Tavola 11.: assegnazione delle chiavi di accesso ai locali dell'ente

COGNOME E NOME	SERVIZIO/FUNZIONE	Struttura di cui si possiede la chiave di accesso	EVENTUALI NOTE
Dal Pozzo Daniela	Responsabile U.O. Sviluppo Organizzativo e Politiche del Personale	Sede Municipale (ingresso laterale) e porta ingresso U.O. Svil.Org. e Pol. Pers.-Piazza Bassi,1	
Bergami Annalisa	Istruttore amministrativo U.O. Sviluppo Organizzativo e Politiche del Personale	porta ingresso U.O. Svil.Org. e Pol. Pers.-Piazza Bassi,1	
Dall'Olio Antonella	Istruttore amministrativo U.O. Sviluppo Organizzativo e Politiche del Personale	porta ingresso U.O. Svil.Org. e Pol. Pers.-Piazza Bassi,1	
Gabriele Mariangela	Istruttore amministrativo U.O. Sviluppo Organizzativo e Politiche del Personale	porta ingresso U.O. Svil.Org. e Pol. Pers.-Piazza Bassi,1	
Capasso Francesco	Sistemi informativi	Ufficio CED – Sala macchine CED	
Tinti Simone	Sistemi informativi	Ufficio CED – Sala macchine CED	
LUI ELISA	Responsabile Area Affari Generali	Sede – P.zza Bassi 1	
Bonino Vincenza	Servizi Amministrativi Area Tecnica	Sede ufficio tecnico via Gramsci 21	
Sunzeri Giuseppina	Servizi Amministrativi Area Tecnica	Sede ufficio tecnico via Gramsci 21	
Focaccia Claudia	Servizi Amministrativi Area Tecnica	Sede ufficio tecnico via Gramsci 21	
Rizzoli Angela	Servizi Amministrativi Area Tecnica e U.O.Commercio	Sede ufficio tecnico via Gramsci 21	



segue

COGNOME E NOME	SERVIZIO/FUNZIONE	Struttura di cui si possiede la chiave di accesso	EVENTUALI NOTE
Bergamini Chiara	Responsabile U.O. Commercio / Servizi Amministrativi	Sede ufficio tecnico via Gramsci 21 e Municipio piazza Bassi	
Rimondini Serena	Responsabile U.O. LL.PP.	Sede ufficio tecnico via Gramsci 21 e Municipio piazza Bassi	
Vannini Maurizio	Lavori Pubblici	Sede ufficio tecnico via Gramsci 21	
Pazzini Marco	Lavori Pubblici	Sede ufficio tecnico via Gramsci 21	
NICODEMO CLAUDIA	RESPONSABILE U.O. PIANIFICAZIONE URBANISTICA	SEDE UFFICIO TECNICO VIA GRAMSCI, 21	
RUSCELLONI FABRIZIO	RESPONSABILE AREA TECNICA	SEDE UFFICIO TECNICO VIA GRAMSCI, 21	
ZERBINI GABRIELE	ASSESSORE SPORT/ LL.PP./ EDILIZIA	SEDE UFFICIO TECNICO VIA GRAMSCI, 21	
BIANCOLI ALBERTO	ASSESSORE ATTIVITÀ PRODUTTIVE/ AMBIENTE	SEDE UFFICIO TECNICO VIA GRAMSCI, 21	
CARINI PAOLO	RESPONSABILE U.O. AMBIENTE	SEDE UFFICIO TECNICO VIA GRAMSCI, 21	
MAZZANTI ALBERTO	ISTRUTTORE TECNICO	SEDE UFFICIO TECNICO VIA GRAMSCI, 21	
ALTILIA LEONARDO	ISTRUTTORE TECNICO	SEDE UFFICIO TECNICO VIA GRAMSCI, 21	
MATTEUZZI ANDREA	ISTRUTTORE TECNICO	SEDE UFFICIO TECNICO VIA GRAMSCI, 21	
ZITA PIERGIORGIO	OPERATORE	SEDE UFFICIO TECNICO VIA GRAMSCI, 21	
BAGLIONI GIOVANNI	AGENTE P.M.	SEDE DEL COMANDO SEDE PALAZZO MUNICIPIO	



segue

COGNOME E NOME	SERVIZIO/FUNZIONE	Struttura di cui si possiede la chiave di accesso	EVENTUALI NOTE
BIGNAMI CRISTINA	COMANDANTE P. M.	SEDE DEL COMANDO SEDE PALAZZO MUNICIPIO	
BORTOLINI VILLIAM	ISPETTORE P.M.	SEDE DEL COMANDO SEDE PALAZZO MUNICIPIO	
BOSELLO MICHELE	AGENTE P.M.	SEDE DEL COMANDO SEDE PALAZZO MUNICIPIO	
CORTESE ALESSIO	AGENTE P.M.	SEDE DEL COMANDO SEDE PALAZZO MUNICIPIO	
DISSETTE PAOLO	ISTRUTTORE AMM.VO	SEDE DEL COMANDO SEDE PALAZZO MUNICIPIO	
FABBRI STEFANO	COMANDANTE P. M.	SEDE DEL COMANDO SEDE PALAZZO MUNICIPIO	
FRANCHINI PATRIZIA	ISPETTORE P.M.	SEDE DEL COMANDO SEDE PALAZZO MUNICIPIO	
FUNICELLI MIRKO	ISPETTORE P.M.	SEDE DEL COMANDO SEDE PALAZZO MUNICIPIO	
MELILLO ATTILIO	AGENTE P.M.	SEDE DEL COMANDO SEDE PALAZZO MUNICIPIO	
SPERA GIANNI	ISPETTORE P.M.	SEDE DEL COMANDO SEDE PALAZZO MUNICIPIO	
VENTURI SIMONA	AGENTE P.M.	SEDE DEL COMANDO SEDE PALAZZO MUNICIPIO	
ZINI RAFFAELLA	AGENTE P.M.	SEDE DEL COMANDO SEDE PALAZZO MUNICIPIO	
MARINA GOTTI	RESPONSABILE AREA SERVIZI ALLA PERSONA/COMUNICAZIONE/URP	CASA BONDI/SEDE MUNICIPALE (SALA CONSIGLIO)	
CASU RAFFAELLA	DIRETTORE ISTITUZIONE SISTER/RESPONSABILE SERVIZI EDUCATIVI	CASA BONDI	

COGNOME E NOME	SERVIZIO/FUNZIONE	Struttura di cui si possiede la chiave di accesso	EVENTUALI NOTE
EMANUELA TUGNOLI	ISTRUTTORE AMMINISTRATIVO ASSEGNATO ISTITUZIONE SISTER	CASA BONDI	
MONICA TARTARINI	RESPONSABILE SERVIZI SOCIALI	CASA BONDI	
TONDINI ROBERTA	ASSISTENTE SOCIALE	CASA BONDI	
RITA RIMONDINI	RESPONSABILE SERVIZI CULTURALI	CASA BONDI/BIBLIOTECA/CENTRO CULTURALE "LA SCUOLA"	
ANNA GIORDANO	ISTRUTTORE AMMINISTRATIVO	CASA BONDI	
MONIA ZINI	ISTRUTTORE AMMINISTRATIVO	CASA BONDI	
ANNA BAIA	ISTRUTTORE AMMINISTRATIVO	CASA BONDI	
ALICE D'AURIA	COLLABORATORE ATTIVITA' UFFICIO	CASA BONDI	
LUANA ANDRAGHETTI	COLLABORATORE ATTIVITA' UFFICIO	CASA BONDI	
ELENA FLAMINI	ISTRUTTORE AMMINISTRATIVO	CASA BONDI/BIBLIOTECA/ CENTRO CULTURALE "LA SCUOLA"	
MARMI MIRANDA	ASSISTENTE BIBLIOTECARIA	CASA BONDI/BIBLIOTECA	
ORSONI LETIZIA	ISTRUTTORE AMMINISTRATIVO	CASA BONDI/BIBLIOTECA	
MARINA SINDACO	OP. CULTURALE COOP. Le macchine celibi	CASA BONDI- MUV	
ANDREA BIAGI	ASSESSORE POLITICHE SOCIALI	CASA BONDI (UFFICIO ASSESSORI)/SEDE MUNICIPALE	
LIONELLO DANILO	CONSILIERE DELEGATO	CASA BONDI (UFFICIO ASSESSORI)	
MARILENA DEL GAUDIO	Assistente di base Consorzio ALDEBARAN	CASA BONDI	



segue

COGNOME E NOME	SERVIZIO/FUNZIONE	Struttura di cui si possiede la chiave di accesso	EVENTUALI NOTE
CLAUDIA ROSSI	Assistente di base Consorzio ALDEBARAN	CASA BONDI	
WALTER GHISI	Assistente di base Consorzio ALDEBARAN	CASA BONDI	
CANGI MARIA	Assistente di base Consorzio ALDEBARAN	CASA BONDI	
PICTOR	Agenzia Pulizia	CASA BONDI - BIBLIOTECA	
GAMBA SERVICE	AGENZIA DI PULIZIA	CENTRO DI DOCUMENTAZIONE VILLANOVIANO E LA SCUOLA DI MARANO	
SAPORI NADIA	Responsabile Servizio URP/Segreteria	Sede – P.zza Bassi 1	
PASQUALI LUCA	Servizio Messi	Sede – P.zza Bassi 1	
BARACANI ANTONELLA	Servizio Messi	Sede – P.zza Bassi 1	
VECCHI SIMONETTA	Servizio Segreteria del Sindaco	Sede - P.zza Bassi 1	
MACCAGNANI COSETTA	Servizi Demografici	Sede – P.zza Bassi 1	
SERMENGHI STEFANO	SINDACO	Sede – P.zza Bassi 1	
ANDREA BIAGI	ASSESSORE POLITICHE SOCIALI	CASA BONDI (UFFICIO ASSESSORI)/SEDE MUNICIPALE	
GIGLIO CONCETTA	ASSESSORE RISORSE UMANE/BILANCIO	Sede – P.zza Bassi 1	
FANTI ANDREA	Segretario Generale	Sede – P.zza Bassi 1	
TUNDO MASSIMILIANO	AREA BILANCIO	ACCESSO LATERALE COMUNE ACCESSO PORTA INTERNA DELL'INGRESSO LATERALE COMUNE ACCESSO UFFICI SERVIZIO BILANCIO	DI FRONTE ALLA PORTA DELLA SALA CONSILIARE



segue

COGNOME E NOME	SERVIZIO/FUNZIONE	Struttura di cui si possiede la chiave di accesso	EVENTUALI NOTE
CIMINO LUISELLA	SERVIZIO BILANCIO	ACCESSO UFFICIO SERVIZIO BILANCIO	
BENEDETTI ROBERTA	SERVIZIO BILANCIO	ACCESSO UFFICIO SERVIZIO BILANCIO	
BONORI MONICA	AREA CONTROLLO DI GESTIONE E TRIBUTI/RESPONSABILE	SEDE COMUNALE (PORTA ESTERNA LATERALE + PORTA DI ACCESSO TRA L'INGRESSO SECONDARIO E L'ATRIO + PORTA DI COMUNICAZIONE TRA UFFICIO TRIBUTI E CORRIDOIO UFFICIO RESPONSABILE DI AREA/ UFFICI DEMOGRAFICI + UFFICIO REPONSABILE DI AREA + PORTA ACCESSO STANZA 15	
GIOSUE'ELETTRA	TRIBUTI- RISCOSSIONE COATTIVA ENTRATE COMUNALI /RESPONSABILE	SEDE COMUNALE (PORTA ESTERNA LATERALE + PORTA DI ACCESSO TRA L'INGRESSO SECONDARIO E L'ATRIO + PORTA DELL'UFFICIO TRIBUTI + PORTA DI COMUNICAZIONE TRA UFFICIO TRIBUTI E CORRIDOIO UFFICIO RESPONSABILE DI AREA E UFFICI DEMOGRAFICI + UFFICIO CIMITERIALE)	
CIOMMI GIADA	CONTROLLO DI GESTIONE/ISTRUTTORE AMMINISTRATIVO	UFFICIO TRIBUTI	
BIANCHI DANIELA	TRIBUTI/ISTRUTTORE AMMINISTRATIVO - CONTABILE	UFFICIO TRIBUTI	
GALLI ELISA	TRIBUTI/ISTRUTTORE AMMINISTRATIVO - CONTABILE	UFFICIO TRIBUTI	

COGNOME E NOME	SERVIZIO/FUNZIONE	Struttura di cui si possiede la chiave di accesso	EVENTUALI NOTE
DONATI DANIELA	TRIBUTI/ COLLABORATORE AMMINISTRATIVO	UFFICIO CIMITERIALE	
MINARDI CLAUDIA	RESPONSABILE U.O. PROVVEDITORATO ECONOMATO	SEDE COMUNALE PORTA SECONDARIA LATERALE CHIAVI INGRESSO SERVIZIO BILANCIO CHIAVI INGRESSO SERVIZIO ECONOMATO	
CLEMENTE CHIARA	ECONOMATO PROVVEDITORATO/ U.O BILANCIO	CHIAVE INGRESSO SERVIZIO BILANCIO CHIAVE INGRESSO SERVIZIO ECONOMATO	
NICODEMO CLAUDIA	RESPONSABILE U.O. PIANIFICAZIONE URBANISTICA	SEDE UFFICIO TECNICO VIA GRAMSCI, 21	
RUSCELLONI FABRIZIO	RESPONSABILE U.O. EDILIZIA PATRIMONIO	SEDE UFFICIO TECNICO VIA GRAMSCI, 21	
CARINI PAOLO	RESPONSABILE U.O. AMBIENTE	SEDE UFFICIO TECNICO VIA GRAMSCI, 21	
MAZZANTI ALBERTO	ISTRUTTORE TECNICO	SEDE UFFICIO TECNICO VIA GRAMSCI, 21	
ALTILIA LEONARDO	ISTRUTTORE TECNICO	SEDE UFFICIO TECNICO VIA GRAMSCI, 21	
MATTEUZZI ANDREA	ISTRUTTORE TECNICO	SEDE UFFICIO TECNICO VIA GRAMSCI, 21	
ZITA GIORGIO	OPERATORE	SEDE UFFICIO TECNICO VIA GRAMSCI, 21	
GUERNELLI ALESSANDRO	INCARICO PROFESSIONALE	SEDE UFFICIO TECNICO VIA GRAMSCI, 21	
Data di aggiornamento: 15/03/2010			

Analisi tecnologica dei dati elettronici

Presentiamo il disegno sintetico della rete del Comune di Castenaso avente lo scopo di rappresentare la rete dell'ente per capirne i punti critici e porre in essere le analisi successive.

Dal punto di vista tecnologico il censimento dei beni da proteggere si identifica in un'attenta analisi della struttura informativa nel suo complesso partendo dal mezzo fisico per arrivare al trasporto ed allo stoccaggio dei dati. L'analisi sarà ripartita in sei aree di intervento:

- ✓ Analisi ambientale.
- ✓ Analisi del sistema di cablaggio.
- ✓ Analisi dell'architettura LAN e WAN.
- ✓ Analisi delle vulnerabilità interne e dell'accesso ai dati.
- ✓ Analisi delle applicazioni.
- ✓ Analisi delle comunicazioni verso Internet.
- ✓ Analisi dei servizi pubblicati sulla rete Internet.

Analisi ambientale

Obiettivo di questa sezione è l'analisi dello stato dei dati informatizzati, con particolare riguardo all'ambiente di ricovero degli stessi.

I dati sono tutti archiviati su server e nessuno di essi è presente sulle stazioni di lavoro PC dei singoli incaricati, se si eccettuano quelli dei posti di lavoro non in rete con il municipio ed i portatili. Tutti i server sono, a loro volta, custoditi nell'area CED.

La sala macchine e l'ufficio dei tecnici informatici sono chiusi a chiave con porte tradizionali e non di sicurezza. Le chiavi sono custodite dagli incaricati nominati nel gruppo "sistemi informativi" (Francesco Capasso e Simone Tinti). Tra la sala macchine e l'ufficio dei tecnici è stato realizzato l'archivio cartaceo dell'ufficio anagrafe con accesso non presidiato.

Il locale, come tutto l'edificio comunale, è protetto da sistema antifurto.

Per prevenire fenomeni di autocombustioni o autospegnimento il locale in cui è situato il CED è condizionato da un impianto in grado di raffreddare il locale. È programmata una temperatura fissa di 22 gradi massimi all'interno dello stesso locale. Il sistema di condizionamento è però ridondato, ma esiste un servizio interno di assistenza, prestato dalla



segue

ClimatZ, per l'impianto in grado di garantire tempi di ripristino dell'ordine di 16 ore lavorative.

Infine l'impianto elettrico del CED è a norma, ed è protetto da un gruppo di continuità in grado di assicurare una autonomia complessiva all'impianto server di circa 15 minuti. Non è presente un gruppo elettrogeno.

Casi particolari: i posti di lavoro delle sedi non collegate alla LAN comunale

In queste sedi i personal computer presenti possono contenere dati personali ed il salvataggio dei dati relativi è in capo agli operatori delle singole sedi.

Analisi del sistema di cablaggio

Tutto il cablaggio è stato realizzato dalle società LGM S.c.r.l. e certificato in categoria 5 enhanced ed è in manutenzione alla medesima ditta.

Gli armadi di cablaggio installati sono:

- due armadi di cablaggio centrale nel Municipio;
- un armadio di cablaggio presso ciascuna delle sedi remote

Tutti i sistemi di cablaggio sono mantenuti dalla società LGM S.c.r.l..

Analisi dell'architettura LAN/WAN

La scelta di analizzare in dettaglio le due architetture può sembrare, a prima vista, superflua, data la possibilità di desumerle dal disegno complessivo del sistema informativo dell'Ente. È utile, però, una scheda di sintesi.

LAN

L'architettura di LAN della sede del Municipio è basata su di una backbone Fast Ethernet, alla quale sono connessi tutti gli switch di piano, realizzata attraverso uno switch che offre anche la connettività fast ethernet verso:

- i server di rete
- gli switch di secondo livello che collegano tutta la periferia di personal computer e stampanti (armadi remoti);

La struttura è comunque piuttosto semplice e provvedono alla sua manutenzione i seguenti fornitori:

1. LGM S.c.r.l. per tutta la parte di apparecchiature attive;
2. il personale interno del CED con switch di ricambio sempre disponibili nei locali del CED per le sedi interessate dal progetto.

Le fibre ottiche collegano la sede del Municipio con le altre sedi del comune. Tutte le fibre in oggetto sono state



segue

collaudate e certificate dall'installatore.

WAN

L'architettura di WAN è realizzata anche attraverso la stesura di fibre proprietarie. In particolare:

1. LGM S.c.r.l. mantiene tutte le connessioni in fibra ottica;
2. HERA, attraverso la consociata Acantho, gestisce l'infrastruttura in fibra ottica nell'ambito della rete regionale LEPIDA verso Internet;

Provvedono alla manutenzione della WAN i seguenti fornitori:

1. Ufficio Tecnico dell'ente (non è chiaramente un fornitore esterno) per quello che riguarda le linee di comunicazione in fibra ed i relativi apparati di interconnessione, linee per le quali è fissato uno SLA (Service Level Agreement) di quattro ore massime per l'intervento;
2. CED dell'ente: non è chiaramente un fornitore esterno, ma è il soggetto che ha disponibili sempre alcuni switch di back-up per sostituire apparecchiature attive eventualmente danneggiate.
3. HERA, attraverso la consociata Acantho, per quello che riguarda la linea in fibra ottica nell'ambito della rete regionale LEPIDA verso Internet;

Analisi delle vulnerabilità interne e dell'accesso ai dati

Specifichiamo ancora che in questa fase stiamo analizzando i dati archiviati su supporto informatico ed elettronico, mentre per quelli di tipo cartaceo rimandiamo l'analisi ad un paragrafo successivo.

Come in precedenza sottolineato, tutti i dati gestiti dall'ente sono archiviati su server, anche le caselle di posta elettronica dei singoli utenti, se si eccettuano i computer portatili: solo in modo transitorio possono lasciare traccia su di un posto di lavoro, ma devono, una volta utilizzata e comunque a fine missione essere ritrasferiti sul server e cancellati dal posto di lavoro, pena l'assunzione da parte dell'operatore di tutte le responsabilità civili e penali derivanti dalla normativa.

Diverso è il discorso per le sedi distaccate, nelle quali non è presente un server, nelle quali non sono presenti, come detto precedentemente, alcun dato.

È importante qui sottolineare le regole di accesso ai dati da parte del personale dell'ente, che possono essere così riepilogate:

1. ogni dipendente ha diritto di accedere solamente ai dati che sono necessari per lo svolgimento delle proprie mansioni;
2. tutti i personal computer dell'ente hanno sistema operativo Windows XP o Windows 2000;



segue

3. ogni dipendente ha uno username, valido finché ha rapporti con l'ente, per l'accesso alla rete dell'ente stesso: lo username permette l'accesso alla rete Windows 200X, che è la base per l'accesso ai dati, e fornisce le credenziali anche per l'accesso ai file server. I server basati su altri sistemi operativi, o le specifiche applicazioni, come la posta elettronica o il software gestionale, richiedono di ridigitare specifici username e password. Viceversa l'accesso ad Internet non è regolamentato da uno username specifico;
4. ad ogni username è associata una password per l'accesso ai server la cui scadenza è fissata in 60 giorni. I server Windows hanno la password a scadenza, mentre per le singole applicazioni deve essere il singolo utente che provvede in autonomia al cambio della password ogni 60 giorni;;
5. in caso di assenza dell'utente, se è necessario accendere la sua stazione di lavoro per condividere la stampante collegata, basta accendere la macchina, la quale viene poi lasciata al Ctrl/Alt/Canc, stato sufficiente per la condivisione della stampante.

Da quanto riassunto si può quindi evincere che l'ente si è dotato di un sistema che offre un buon livello di sicurezza nell'accesso ai dati. E' fatto comunque divieto a chiunque di portare all'esterno dati gestiti dal proprio servizio di appartenenza, sotto una qualunque forma, ad eccezione dei casi autorizzati previsti dal manuale di istruzione degli incaricati.

I Consiglieri Comunali e il gruppo del Consiglio Comunale hanno a disposizione un PC che usufruisce del collegamento ad Internet della rete del Municipio; detti utenti hanno accesso al Dominio Windows dell'Amministrazione con diritti propri.

La rete della Biblioteca, non ha proprio accesso ad Internet fisico, ma virtuale, attraverso una subnet specifica, separata dalla LAN dell'ente.

Alla Lan così separata della biblioteca potranno accedere anche:

- i cittadini utenti della biblioteca

Analisi delle applicazioni: regola 19.8 dell'Allegato B al Codice

Chi redige il documento ha approfondito lo stato dell'arte delle applicazioni gestionali installate nel comune e, anche a seguito di un confronto avuto con l'Avvocato Stefano Orlandi, in team con il quale viene redatto questo documento, esperto ed autore di pubblicazioni sull'argomento specifico, dobbiamo fare le seguenti considerazioni che valgono per le applicazioni software presenti nell'ente.

Tali applicazioni infatti paiono conformi ai seguenti punti del d.lgs. 196/2003 denominato "Codice sulla tutela dei dati personali", anche in relazione agli aggiornamenti effettuati:

1. Titolo III Art. 22 comma 6 recita: "I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.
2. Titolo III Art. 22 comma 7 recita: "I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.

Il software, inoltre, pare conforme alle seguenti regole delle misure minime (allegato B del d.lgs. in oggetto):

1. Art. 16 recita: I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
2. Art. 17 recita: Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale

Tutti i dati comunali sono infatti protetti da sistema antivirus. L'amministratore ha predisposto un sistema antivirus sia sui client e sui server, sistema che dovrebbe ridurre al minimo tale rischio, ma che non può eliminarlo totalmente come risaputo.

Presentiamo di seguito un elenco di dettaglio dei software installati presso l'Ente

Tavola 12.riepilogativa del censimento dei software applicativi informatici che rientrano nel piano di sicurezza dell'ente

Prog.	Denominazione	Descrizione	Application Server (H=Hardware V=Vmware)		Server RDBMS (H=Hardware V=Vmware)	
1.	Iride Web	Gestione delibere e determinazioni dirigenziali Gestione Registrazioni posta in arrivo e posta in partenza Registrazione atti da notificare Registrazione atti da pubblicare	Server10	H	Server16	H
2.	Garsia	Gestione dei servizi socio-sanitari integrati anziani	Server10	H	Server10	H
3.	Sosia	Gestione Rette Scolastiche e Anziani	Server10	H	Server16	H
4.	Gradus	Gestione graduatorie	Server10	H	Server16	H
5.	Time @ Web	Rilevamento ed elaborazione Presenze	Server15	H	Server16	H
6.	Veritas	Gestione del Backup di tutti i dati	BckServer	H	BckServer	H
7.	Lotus notes	Gestione posta elettronica	Server01	V	Server01	V
8.	MailCleaner	blocca virus, spam e codici maligni nella posta elettronica (programma Opensource che integra SpamAssassin, Clamav Antivirus, whitelist Razor)	Mailcleaner	V	Mailcleaner	V

Prog.	Denominazione	Descrizione	Application Server (H=Hardware V=Vmware)		Server RDBMS (H=Hardware V=Vmware)	
9.	CityWare	Gestione Ici, Tarsu, Tosap	(Client Locali con aggiornamento centralizzato da Server10)	H	Server16	H
10.	Perseo	Gestione retribuzioni del personale	Server10	H	Server16	H
11.	Kronos	Visualizzazione web dei cedolini paga per i dipendenti	Server10	H	Server16	H
12.	SIT	Sistema Informativo territoriale	CAST0674	H	file10.sanlazzaro.local	H
13.	Aedilis	Gestione concessioni edilizie	Server10	H	Server16	H
14.	STR Win32	Gestione contabilità cantieri	Server10	H	Server16	H
15.	Arcadia	Gestione anagrafe, elettorale, stato civile popolazione residente e italiani residenti all'estero (A.I.R.E.)	Server10	H	Server16	H
16.	Concilia	Gestione contravvenzioni al codice della strada ed ai regolamenti comunali	Server15	H	Server16	H
17.	eZPA	Piattaforma tecnologica sito internet comunale (Opensource CMS + PostgreSql)	harpstrong	V	harpstrong	V
18.	GLPI	Gestione HelpDesk per chiamate al CED (Opensource con interfaccia web)	helpdesk	V	helpdesk	V

Prog.	Denominazione	Descrizione	Application Server (H=Hardware V=Vmware)		Server RDBMS (H=Hardware V=Vmware)	
19	Socrate	Gestione accertamenti effettuati dalle Volanti PM	Server10	H	Server16	H
20	SigmaInfo6	Gestione Cimiteriale	Server10	H	Server10	H
21	AnagAIRE	Gestione e invio dati AIRE al ministero dell'interno	Server10	H	Server10	H
22	Debian + Squid, Iptables, Snort, Apache2, OpenVPN	Firewall Interno con funzioni di : 1)Proxy Server per la navigazione degli utenti 2)Reverse Proxy per la pubblicazione di servizi OnLine 3)Intrusion Detection System(IDS) 4)Gestione VPN per collegamento tra comuni dell'associazione	Mammut	H		
23	Debian + Iptables e Snort	Firewall Esterno esposto su internet con funzioni di Intrusion Detection System(IDS)	Bisonte	H		
24	Debian + OpenVPN	Gestione VPN per assistenza remota dall'esterno sui programmi gestionali in uso	Ocipete	V		
25	Windows Update Services	Distribuzione centralizzata degli aggiornamenti Microsoft	Serverwus	V	Serverwus	V
26	CityTown	Calcolo ICI OnLine	websrvcitytown	V	websrvcitytown	V
27	Cessione fabbricati	Denuncia antiterrorismo	Server10 + H	V	Server10 + H	V
Data di aggiornamento: 15/03/2010						

Analisi delle comunicazioni verso Internet

Tutte le comunicazioni verso Internet passano attraverso il collegamento con la rete regionale LEPIDA: tale connessione è basata su tecnologia in fibra ottica a 100 MBit nominali presente nella sede del Municipio. L'ente si è dotato di tutta la strumentazione necessaria per ridurre al minimo i rischi di intrusione nonché di fuoriuscite di dati non autorizzate verso la rete.

Per prima cosa è opportuno presentare sinteticamente la struttura di comunicazione, meglio descritta dall'immagine presentata in precedenza:

- il server di posta elettronica è interno e completamente gestito dal CED;
- tutti gli utenti autorizzati possono navigare in Internet;
- la rete interna è divisa dalla rete pubblica da due firewall, che gestiscono anche i log di connessione degli utenti (della cui esistenza gli utenti sono informati nel manuale di formazione utente), nel quale sono fissate le seguenti regole:
 - o porte aperte in uscita: http, https, smtp, pop3, ftp (aperta solo per gli utenti del CED);
 - o porte aperte in ingresso: smtp, pop3, imap e posta elettronica via reverse proxy su porta 80

E' necessario ora riepilogare i servizi attivi:

- tutti gli utenti dotati di personal computer hanno la posta elettronica, con possibilità di inviare/ricevere allegati: questo servizio è funzionale allo svolgimento della propria mansione;
- è presente un filtro sui tipi di allegato: sono negati tutti i contenuti eseguibili e file audio/video
- navigazione in Internet secondo quanto detto sopra, ovvero con logging delle attività svolte secondo quanto stabilito nel disciplinare Internet redatto ed aggiornato annualmente;

Una parte consistente di quanto sopra riportato è riaffermato nella "Politica di sicurezza dell'ente", che sarà illustrata successivamente.

Analisi dei servizi pubblicati sulla rete Internet

I servizi pubblicati sulla rete Internet sono numericamente ristretti, ma vale ugualmente la pena citarli per meglio comprendere il loro impatto sulla sicurezza dei dati:

1. Il primo servizio pubblicato, ma di scarsa importanza ai fini della sicurezza, è dato dalle pagine web di presentazione dell'ente, raggiungibili al link www.comune.castenaso.bo.it.



segue

2. ICI web servizio per il calcolo on-line dell'ICI
3. Mailing list del comune
4. Web mail per gli utenti interni
5. Garsia invece è un servizio di pubblicazione, verso la ASL Città di Bologna via Internet, di dati: i dati sono aggiornati dagli operatori del comuni ed il sistema provvede ad aggiornarli nella sede dell'ASL. I dati sono oggetto di back-up sia all'interno dell'ente che all'interno dell'ASL
6. Pubblicazione del servizio di consultazione per il cittadino delle immagini riprese dai dispositivi photored installati ai semafori. Il cittadino tramite i dati presenti sul verbale che gli è stato notificato può accedere via web alle foto che lo riguardano

Non sono presenti altri servizi applicativi pubblicati.



Analisi dei dati cartacei

Analisi ambientale

Le operazioni di trattamento dei dati cartacei avvengono negli uffici e/o reparti dove lavorano gli incaricati. Ogni ufficio è dotato di contenitori muniti di chiave nei quali riporre i dati personali sensibili e giudiziari, come indicato dal manuale di istruzioni fornito agli incaricati.

Ogni ufficio è ad accesso regolamentato, nel senso che le porte della sede di riferimento si aprono solo grazie al “via libera” fornito dalla chiave in possesso dei capi ufficio, come evidenziato dalla tabella relativa. I singoli incaricati possono anche accedere, dietro autorizzazione del responsabile di reparto/ufficio, in ambienti diversi da quelli di lavoro ordinario.

Analisi delle vulnerabilità interne e dell’accesso dei dati

I rischi a cui sono soggetti i dati cartacei trattati dall’ente sono quelli tradizionali:

- sottrazione di documenti da parte del personale
- mancata reposizione dei dati trattati sotto chiave, quindi la mancata osservazione delle istruzioni impartite agli incaricati.

Le criticità dei beni informatici preposti al trattamento dei dati elettronici

L'analisi della criticità dei beni riguarda esclusivamente la dotazione informatica preposta al trattamento dei dati elettronici.

Occorre precisare che l'analisi è indirizzata a misurare la criticità della disponibilità dei dati, di conseguenza oggetto di analisi sono i beni informatici in quanto consentono la disponibilità dei dati stessi.

Tale analisi è effettuata sotto due punti di vista:

- il *fault tolerance*: questa analisi, che nel presente lavoro sarà particolarmente approfondita, si può desumere implicitamente dalla lettura dell'Allegato B del d.lgs n. 196/03 "Codice in materia di protezione dei dati personali" dove si sancisce la necessità di garantire la "disponibilità dei dati";
- il *disaster recovery*: questa seconda analisi rientra tra le misure minime dell'Allegato B del d.lgs n.196/03 "Codice in materia di protezione dei dati personali".

Il *fault tolerance*

La strategia di *fault tolerance* è data da tutti quegli accorgimenti che permettono di garantire la continuità del servizio informatico. Tale strategia assume notevole rilevanza nel trattamento dei dati dell'ente e soprattutto nelle necessità di garantire la continuità del servizio. Il Comune di Castenaso è infatti una realtà che offre un pubblico servizio. Di conseguenza tutti i fattori volti a garantire al massimo la continuità di lavoro, rivestono una importanza decisiva o, addirittura, vitale.

Per procedere a questa prima analisi occorre innanzitutto definire il livello di criticità di ciascun bene informatico (da ora in poi denominato *device*), per poterlo poi classificare e successivamente definire le azioni da intraprendere per affrontare i possibili fermi macchina.

E' possibile ipotizzare una scala di criticità che va da 1 a 4 così definita:

1. *minimo*: i device possono stare fermi anche una settimana senza che si riscontrino problemi all'intero sistema informativo;
2. *intermedia*: il device può stare fermo per una settimana senza problemi all'intero sistema informativo, tranne che in periodi critici di eccesso di lavoro, nel quale le possibilità di fermo si riducono a 8 ore lavorative;
3. *alta*: il device non può, in qualunque situazione stare fermo per più di 8 ore lavorative (24 ore solari);
4. *critica*: il device non può stare fermo per più di 4 ore lavorative.

Occorre, in primo luogo, definire la criticità di tutti i device sotto elencati per elaborare una strategia di intervento efficace a coprire le esigenze di *fault tolerance*.

Tavola 13.: Tabella riepilogativa dei device presenti nell'ente: censimento dei beni informatici

Servizi funzionali										
Device	File server	Altri server	DB Server gestionale	E-mail	Apps gestionali	Servizi di gestione	Router o switch	Marca	S.O	F.T.
Municipio										
SERVER01				3				Vmware	Windows NT 4.0 Sp6a	
SERVER02		3			3	Printer Server		Vmware	Windows 2000 server SP4	
SERVER10	4				4			HP ProLiant DL380 G3	Windows 2000 server SP4	Raid 5
SERVER15		3			3	Terminal Server		Fujitsu Siemens Primergy	Windows 2000 server SP4	Raid 5
SERVER16			4					Fujitsu Siemens Primergy	Windows 2003 Server SP1	Raid 5
MAMMUT		4				4		Assemblato	Linux Debian	Raid 5
BISONTE		4				4		HP	Linux Debian	Raid 5
SVRCASTENASO		2				Vmware Server		HP ProLiant DL380 G3	Windows 2000 server SP4	Raid 5
ADCAST02						4		Vmware	Windows 2000 server SP4	
ADCAST04						4		Vmware	Windows 2000 server SP4	
BCKSERVER						3		IBM Netfinity 3000	Windows 2000 Professional SP4	Raid 1
HELPDESK		2	2					Vmware	Linux Ubuntu Server 6.06	
LDAPBIBLIO						2		Vmware	Linux Ubuntu Server 7.10	
MAILCLEANER		4						Vmware	Linux Debian	
OCIPETE		2						Vmware	Linux Debian	
SERVERWUS		1						Vmware	Windows 2003 Server SP1	
WEBSRVCITYTOWN	2	2						Vmware	Windows 2000 server SP4	
CASTCEICNSD		3						Vmware	Windows 2000 Professional SP4	



segue

Servizi funzionali										
Device	File server	Altri server	DB Server gestionale	E-mail	Apps gestionali	Servizi di gestione	Router o switch	Marca	S.O	F.T.
Virtuoso01		4				X		Assemblato	VMware ESXi 3.5	
Virtuoso02		4				X		Assemblato	VMware ESXi 3.5	
EleOnLine		2 EleOnLine Web						Vmware	Debian Linux	
CastBackupSRV		2				SyncToy Microsoft		Vmware	Windows XP SP3	
MulteWeb		3				X Tomcat		Vmware	Linux Debian 5	
CAST0817	3							Lacie	NAS	Raid 1
CAST0818	3							Lacie	NAS	Raid 5
Switch 1 Armadio CED							4	Allied Telesyn	n.a.	Nessuno
Switch 2 Armadio CED							4	Allied Telesyn	n.a.	Nessuno
Switch 3 Armadio CED							4	3Com	n.a.	Nessuno
Switch Armadio Server							4	HP procure	n.a.	Nessuno
Ufficio tecnico										
Switch vari							4	Vari	n.a.	Nessuno
Polizia Municipale										
Switch vari							4	Vari	n.a.	Nessuno
Servizi Sociali										
Switch vari							4	Vari	n.a.	Nessuno
Biblioteca										
Switch vari							4	Vari	n.a.	Nessuno
Data di aggiornamento: 15/03/2010										

Legenda

I numeri indicati nelle celle evidenziate in giallo indicano il fattore di criticità riepilogato sede per sede (i numeri sono assegnati sulla base della scala di criticità prima esplicitata).

F.T. sta per Fault Tolerance

Con i simboli rossi è indicato, invece, l'impatto che un eventuale fault del device può avere sui servizi in ordinata.

Il disaster recovery

Analizzare le problematiche di disaster recovery è molto più complesso in quanto i problemi da affrontare sono molteplici:

Innanzitutto bisogna rifare un'analisi di criticità orientata specificamente ai server, ed una orientata alle linee di



segue

comunicazione, in quanto i termini sono differenti da quelli usati per lo studio precedente: possiamo però rifarci all'elenco sopra riportato per un censimento dei server e dei collegamenti WAN.

Occorre, innanzitutto, definire i fattori di criticità relativi alle problematiche di disaster recovery allo scopo di stabilire una scala di importanza dei dati/applicazioni/conessioni, in quanto non è possibile pensare di assegnare lo stesso fattore di importanza a tutti i servizi. Anche in questo caso è congeniale ipotizzare una scala di criticità che procede da 1 a 2 così definita:

1. *minimo*: questi server/link non contengono dati d'importanza vitale per l'ente, o, in altre parole, contengono dati per i quali è possibile aspettare le normali operazioni di *restore*, dai nastri di back-up che saranno depositati "al sicuro" con periodicità da definire, o di *ripristino* da normali operazioni di assistenza;
2. *critica*: questi server/link contengono dati d'importanza vitale per l'attività produttiva dell'ente e devono essere ripristinati immediatamente in una locazione diversa da quella che ha subito il disastro, con uno switch il più possibile automatizzato;

Occorre quindi definire la criticità di tutti i device sotto elencati per elaborare una strategia di intervento efficace a coprire le esigenze di disaster recovery.

Tavola 14.: Tabella riepilogativa dei fattori di criticità per il servizio di disaster recovery

Servizi funzionali										
Device	File server	Altri server	DB Server gestionale	E-mail	Apps gestionali	Servizi di gestione	Router o switch	Marca	S.O	F.T.
Municipio										
SERVER01				2				Vmware	Windows NT 4.0 Sp6a	
SERVER02		1			1	Printer Server		Vmware	Windows 2000 server SP4	
SERVER10	2				2			HP ProLiant DL380 G3	Windows 2000 server SP4	Raid 5
SERVER15		2			2	Terminal Server		Fujitsu Siemens Primergy	Windows 2000 server SP4	Raid 5
SERVER16		👤	2			👤		Fujitsu Siemens Primergy	Windows 2003 Server SP1	Raid 5
MAMMUT		2		👤		X		Assemblato	Linux Debian	Raid 5
BISONTE		2		👤		X		HP	Linux Debian	Raid 5
SVRCASTENASO				👤		Vmware Server		HP ProLiant DL380 G3	Windows 2000 server SP4	Raid 5
ADCAST02	👤	👤	👤	👤	👤	2		VMware	Windows 2000 server SP4	



segue

Servizi funzionali										
Device	File server	Altri server	DB Server gestionale	E-mail	Apps gestionali	Servizi di gestione	Router o switch	Marca	S.O	F.T.
ADCAST04				☺☺☺		1		Vmware	Windows 2000 server SP4	
BCKSERVER	☺☺☺		☺☺☺	☺☺☺		1		IBM Netfinity 3000	Windows 2000 Professional SP4	Raid 1
HELPDESK		1	1					Vmware	Linux Ubuntu Server 6.06	
LDAPBIBLIO		1				OpenLDAP		Vmware	Linux Ubuntu Server 7.10	
MAILCLEANER		2						Vmware	Linux Debian	
OCIPETE		2						Vmware	Linux Debian	
SERVERWUS		1						Vmware	Windows 2003 Server SP1	
WEBSRVCITYTOWN	1	1						Vmware	Windows 2000 server SP4	
CASTCEICNSD		2						Vmware	Windows 2000 Professional SP4	
Virtuoso01		2				X		Assemblato	VMware ESXi 3.5	
Virtuoso02		2				X		Assemblato	VMware ESXi 3.5	
EleOnLine		1 EleOnLine Web						Vmware	Debian Linux	
CastBackupSRV		1				SyncToy Microsoft		Vmware	Windows XP SP3	
MulteWeb		1				X Tomcat		Vmware	Linux Debian 5	
CAST0817	2							Lacie	NAS	Raid 1
CAST0818	2							Lacie	NAS	Raid 5
Switch 1 Armadio CED	☺☺☺	☺☺☺	☺☺☺	☺☺☺	☺☺☺	☺☺☺	X	Allied Telesyn	n.a.	Nessuno
Switch 2 Armadio CED	☺☺☺	☺☺☺	☺☺☺	☺☺☺	☺☺☺	☺☺☺	X	Allied Telesyn	n.a.	Nessuno
Switch 3 Armadio CED	☺☺☺	☺☺☺	☺☺☺	☺☺☺	☺☺☺	☺☺☺	X	3Com	n.a.	Nessuno
Switch Armadio Server	☺☺☺	☺☺☺	☺☺☺	☺☺☺	☺☺☺	☺☺☺	X	HP procurve	n.a.	Nessuno
Ufficio tecnico										
Switch vari							2	Vari	n.a.	Nessuno
Polizia Municipale										
Switch vari							2	Vari	n.a.	Nessuno
Servizi Sociali										
Switch vari							2	Vari	n.a.	Nessuno



segue

Servizi funzionali										
Device	File server	Altri server	DB Server gestionale	E-mail	Apps gestionali	Servizi di gestione	Router o switch	Marca	S.O	F.T.
Biblioteca										
Switch vari							2	Vari	n.a.	Nessuno
Data di aggiornamento: 15/03/2010										

Legenda

I numeri indicati nelle celle evidenziate in giallo indicano il fattore di criticità riepilogato sede per sede (i numeri sono assegnati sulla base della scala di criticità prima esplicitata).

F.T. sta per Fault Tolerance

Con i simboli blu è indicato, invece, l'impatto che una mancanza del device può avere sui servizi in ordinata.

L'analisi dei rischi a cui possono essere soggetti i dati elettronici e i dati cartacei: regola 19.3 dell'Allegato B al Codice

In linea con l'art. 35, Capo I, Titolo V del d.lgs. n. 196/2003 che *“impone di ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta”* si procede analizzando i rischi a cui sono soggetti i dati informatici ed i dati cartacei trattati dagli incaricati dell'ente.

Per ciò che concerne le azioni intraprese per fronteggiare tali rischi si rimanda al capitolo relativo al *Documento Programmatico per la sicurezza dei dati*.

Analisi dei rischi dei dati elettronici

I rischi ai quali possono essere soggetti i dati residenti sugli elaboratori presenti nell'ente, già precedentemente inventariati, sono i seguenti:

- Accesso indebito alle risorse sia da parte di personale interno non autorizzato, che da parte di “pirati” esterni.
- Rischi connessi alla trasmissione dei dati.
- Perdita dei dati e quindi perdita della loro integrità fisica.
- Errori operativi volti a minare l'integrità logica dei dati.
- Azioni dolose.
- Manomissioni o furti.
- Eventi dannosi o disastrosi.

Presentazione sintetica dei rischi a cui sono soggetti i dati elettronici trattati dal Comune di Castenaso.

Tavola 15.: I rischi a cui sono soggetti i dati elettronici trattati dal Comune di Castenaso sono di seguito riepilogati:

Rischio	Dettaglio	Gravità stimata	Probabilità di accadimento
<u>Accesso indebito alle risorse da parte di utenti interni all'ente</u>	• Accesso alle banche dati non autorizzato. • Copie non autorizzate dei dati per il trasporto all'esterno dell'ente	☐ Alta ☐ Alta	☐ Bassa ☐ Media
<u>Comportamenti degli operatori</u>	• Furto di credenziali di autenticazione • carenza di consapevolezza, disattenzione o incuria • comportamenti sleali o fraudolenti • errore materiale	☐ Alta ☐ Alta ☐ Alta ☐ Media	☐ Bassa ☐ Bassa ☐ Bassa ☐ Bassa
<u>Eventi relativi agli strumenti</u>	• azione di virus informatici o di codici malefici • spamming o altre tecniche di sabotaggio • malfunzionamento, indisponibilità o degrado degli strumenti	☐ Alta ☐ Alta ☐ Media	☐ Media ☐ Media ☐ Media
<u>Eventi relativi al contesto</u>	• accessi non autorizzati a locali/reparti ad accesso ristretto • Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ...)	☐ Media ☐ Alta	☐ Bassa ☐ Media



segue

Rischio	Dettaglio	Gravità stimata	Probabilità di accadimento
<u>Sicurezza nelle trasmissioni</u> dei dati	- Tentativi di carpire i dati che vengono inviati all'ente da parte di pirati esterni. - Tentativi di carpire i dati che vengono spediti dal Comune di Castenaso da parte di pirati esterni. - Rischio di invio dati a destinatari sbagliati. - Tentativi di intrusione nella rete interna dell'ente. dall'esterno, da Internet, da sedi di comuni collegati via linee telefoniche all'ente e da parte di pirati esterni.	☐ Alta ☐ Alta ☐ Bassa ☐ Alta	☐ Media ☐ Media ☐ Bassa ☐ Media
<u>Rischi circa l'integrità fisica</u> dei dati	- Cancellazione involontaria/accidentale dei dati. - Servizi di back-up non andati a buon fine.	☐ Bassa ☐ Bassa	☐ Bassa ☐ Bassa
<u>Rischi circa l'integrità logica</u> dei dati	- Incongruenze fra i dati. - Le applicazioni software in uso che creano disallineamenti.	☐ Bassa ☐ Bassa	☐ Bassa ☐ Bassa
Rischi <u>manomissioni o furti o azioni dolose</u>	- Manomissioni del CED. - Furti di dati sia dagli elaboratori, che dagli elaboratori stessi.	☐ Alta ☐ Alta	☐ Bassa ☐ Bassa
<u>Eventi dannosi o disastrosi</u>	Incendio.	☐ Alta ☐ Impredicibile	☐ Media ☐ Alta



segue

Analisi dei rischi dei dati cartacei

I rischi ai quali possono essere soggetti i dati cartacei presenti nell'ente sono i seguenti:

- Accesso indebito alle risorse sia da parte di personale interno non autorizzato.
- Rischi connessi alla trasmissione dei dati.
- Perdita dei dati e quindi perdita della loro integrità fisica.
- Furti e azioni dolose.
- Eventi dannosi o disastrosi.
- Rischi connessi alla procedura di eliminazione di dati erroneamente stampati.

Presentazione sintetica dei rischi a cui possono essere soggetti i dati cartacei trattati dall'ente

Tavola 16.: I rischi a cui possono essere soggetti i dati cartacei trattati dall'ente possono essere così riepilogati:

Rischio	Dettaglio	Gravità stimata	Probabilità di accadimento
<u>Accesso indebito alle risorse da parte di utenti interni all'ente</u>	• Accesso alle banche dati non autorizzato. • Copie non autorizzate dei dati per il trasporto all'esterno dell'ente	☐ Alta ☐ Alta	☐ Bassa ☐ Media
<u>Comportamenti degli operatori</u>	• Carenza di consapevolezza, disattenzione o incuria • comportamenti sleali o fraudolenti • errore materiale	☐ Alta ☐ Alta ☐ Media	☐ Bassa ☐ Bassa ☐ Bassa
<u>Eventi relativi al contesto</u>	• accessi non autorizzati a locali/reparti ad accesso ristretto • Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ...)	☐ Media ☐ Alta	☐ Bassa ☐ Media



segue

Rischio	Dettaglio	Gravità stimata	Probabilità di accadimento
<u>Sicurezza nelle trasmissioni</u> dei dati	Rischio di invio dati a destinatari sbagliati.	☐ Bassa	☐ Bassa
<u>Rischi circa l'integrità fisica</u> dei dati	Cancellazione involontaria/accidentale dei dati	☐ Bassa	☐ Bassa
<u>Eventi dannosi o disastrosi</u>	Incendio.	☐ Alta ☐ Impredicibile	☐ Media ☐ Alta
<u>Rischi connessi alla procedura di eliminazione di dati erroneamente stampati</u>	Mancata distruzione dei dati erroneamente stampati dagli incaricati	☐ Alta	☐ Bassa

L'analisi dei sistemi di videosorveglianza

In linea con quanto previsto dal Garante per la protezione dei dati personali, nonché dalla Convenzione europea sui diritti dell'uomo, il trattamento dei dati attraverso sistemi di videosorveglianza avviene rispettando i seguenti principi legislativi:

- principio di liceità: non sono ammissibili interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e di tutti gli altri luoghi ai quali è riconosciuta analoga tutela (tali limitazioni si aggiungono a quelle già previste dal c.p. in materia di intercettazioni di comunicazioni e di conversazioni);
- principio di necessità: un sistema di videosorveglianza introduce un vincolo per il cittadino in termini di limitazioni o condizionamenti, di conseguenza si deve escludere ogni uso superfluo o eccessivo;
- principio di proporzionalità: l'ente o l'impresa deve valutare innanzitutto il grado di rischio in cui può incorrere e adottare un sistema di videosorveglianza solo quando le altre misure si rivelano insufficienti; la soluzione che porta all'adozione di un sistema di videosorveglianza non deve rispondere a meri criteri di risparmio o di semplicità;
- principio di finalità: con l'introduzione di sistemi di videosorveglianza possono essere perseguite solo finalità trasparenti e portate opportunamente a conoscenza del pubblico mediante comunicazioni o cartelli, escludendo qualsiasi finalità generiche o indeterminate.

Tavola 17.: Tabella riepilogativa dei sistemi di videosorveglianza

Progressivo	Dislocazione e scopo	Registrazione
1.	Sede del Municipio per il controllo degli accessi al palazzo comunale	SI *
2.	Sede Polizia Municipale	SI *
3.	Cimitero Comunale	SI *
4.	Via Di Vittorio	SI *
5.	Via Cà dell'Orbo	SI*
6.	Via Golinelli	SI*
7.	Via Tosarelli 205	SI*
8.	Via Nasica 20	SI*



segue

9.	Via Risorgimento 1	Sì*
10.	Via Bentivogli 36	Sì*
11.	Piazza Zapelloni	Sì*
12.	Biblioteca Comunale	Le videocamere non sono al momento collegate alla centralina
Data di aggiornamento: 15/03/2010		

* Le registrazioni dei dati sono conservate presso il Comando di Polizia Municipale per un periodo di 7 giorni.

Adempimenti ottemperati

DOVERE DI INFORMAZIONE

Gli interessati sono informati con formule sintetiche, ma chiare e senza ambiguità, che stanno per accedere o che si trovano in una zona videosorvegliata e dell'eventuale registrazione anche se si tratta di eventi, di spettacoli pubblici o di attività pubblicitarie.

MISURE DI SICUREZZA

Quando i dati vengono conservati sono previsti, all'interno della struttura, diversi livelli di accesso al sistema e di utilizzo delle informazioni, avendo riguardo anche agli interventi ordinari e straordinari di manutenzione. La risposta adottata al rischio che si verifichino abusi è stata l'introduzione di una "doppia chiave" fisica o logica che consente un'immediata ed integrale visione delle immagini solo in caso di necessità.

Sono previste iniziative periodiche di formazione degli incaricati sui doveri, sulle garanzie e sulle responsabilità, sia nel momento dell'introduzione del sistema di videosorveglianza, sia in sede di modifica dello stesso.

Le misure di sicurezza riducono al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta.

DURATA DELL'EVENTUALE CONSERVAZIONE

In linea con il principio di proporzionalità anche l'eventuale conservazione temporanea è commisurata al grado di indispensabilità e per il solo tempo necessario a raggiungere la finalità perseguita.

La conservazione è a poche ore o, al massimo, alle 24 ore successive alla rilevazione, fatte salve speciali esigenze in relazione a festività o chiusura di uffici, a richieste dell'autorità giudiziaria, a speciali esigenze tecniche o per la particolare rischiosità dell'attività svolta dal titolare. In quest'ultimo caso il termine più ampio di conservazione dei dati non può comunque superare la settimana.

La definizione della politica di sicurezza dell'ente

E' la fase organizzativa più importante e delicata da affrontare, che vede coinvolti il redattore del presente progetto con il responsabile di progetto incaricato dal Comune di Castenaso.

Occorre precisare che per quanto riguarda la gestione dei dati sensibili su supporto cartaceo vale la regola generale, condivisa dall'intera organizzazione ed opportunamente esplicitata nel manuale di istruzione dei diversi incaricati, in base alla quale alla fine di ciascun trattamento autorizzato devono essere riposti sotto chiave nei relativi archivi.

Si procede invece all'analisi dei dati elettronici che si articola in 4 punti:

1. *Chi-fa-cosa dentro*, ovvero chi, all'interno dell'organizzazione ha diritto di accedere a dati (digitali o cartacei), in che orari, con che diritti, che server ha diritto di utilizzare, quali applicazioni, ecc.
2. *Chi-fa-cosa fuori*, ovvero chi ha diritto di uscire verso Internet, verso i clienti, partners, fornitori, che ha diritto di usare un modem, chi ha diritto di fare qualunque cosa che, nell'esercizio delle proprie funzioni, entri in relazione con il mondo esterno.
3. *Chi, interno, fa cosa da fuori* ovvero chi, membro dell'organizzazione, ha necessità di accedere dall'esterno alla rete dell'ente con che diritti e per fare cosa.
4. *Chi, esterno, può fare cosa da fuori*, ovvero chi esterno all'organizzazione, come un fornitore o un partner, può fare cosa nel momento in cui accede ai sistemi informativi, digitali o cartacei, della organizzazione.
 - a. Rapporti con aziende esterne all'organizzazione assimilabili a titolari del trattamento.

Chi-fa-cosa dentro

In questa fase si analizza chi, all'interno dell'organizzazione ha diritto di accedere a dati elettronici, in che orari, con che diritti, che server ha diritto di utilizzare, quali applicazioni, ecc..

Legenda: R sta per **read** (diritto di lettura) e W sta per **write** (diritto di scrittura).

Tavola 18.: *chi-fa-cosa dentro*

Gruppi	Server	Diritti	Orari
Segretario Generale	File Server	R/W per la directory di area e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione

Gruppi	Server	Diritti	Orari
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione
Sviluppo Organizzativo e Politiche del Personale	File Server	R/W per la directory di area e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione
Area Tecnica: Edilizia – Patrimonio - Suap	File Server	R/W per la directory di area e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione
Area Tecnica: Servizio Lavori Pubblici	File Server	R/W per la directory di area e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione



segue

Gruppi	Server	Diritti	Orari
	Servizi di gestione	Nessuno	Nessuna limitazione
Area Tecnica: Pianificazione territoriale	File Server	R/W per la directory di area e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione
Area Tecnica: Servizi Ambientali	File Server	R/W per la directory di area e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione
Area Tecnica: Commercio Servizi Amm.vi	File Server	R/W per la directory di area e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione



segue

Gruppi	Server	Diritti	Orari
Polizia Municipale	File Server	R/W per la directory di area e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione
Area Servizi alla Persona e Comunicazione ed Istituzione Sister	File Server	R/W per la directory di area e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione
Area Affari Generali: URP Segreteria e Ufficio Legale	File Server	R/W per la directory di area e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione



segue

Gruppi	Server	Diritti	Orari
Area Affari Generali: Servizi demografici	File Server	R/W per la directory di area e “amministratore” per le altre	Nessuna limitazione
	Altri server	Amministratore	Nessuna limitazione
	DB Server gestionale	Amministratore	Nessuna limitazione
	E-Mail server	Amministratore	Nessuna limitazione
	Applicazioni gestionali	Amministratore	Nessuna limitazione
	Servizi di gestione	Amministratore	Nessuna limitazione
Sistemi Informativi	File Server	R/W per la directory di area e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	R/W	Nessuna limitazione
Area Bilancio: Servizio Bilancio	File Server	R/W per la directory di area e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione



segue

Gruppi	Server	Diritti	Orari
Area Bilancio: U.O. Provveditorato – Economato	File Server	R/W per la directory di area e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione
Area Controllo di Gestione e Tributi	File Server	R/W per la directory di area e nessuno per le altre	Nessuna limitazione
	Altri server	R	Nessuna limitazione
	DB Server gestionale	R/W	Nessuna limitazione
	E-Mail server	R/W	Nessuna limitazione
	Applicazioni gestionali	R/W	Nessuna limitazione
	Servizi di gestione	Nessuno	Nessuna limitazione

Chi-fa-cosa fuori

In questa fase ci si sofferma su chi ha diritto di uscire verso Internet, verso i clienti, partners, fornitori, che ha diritto di usare un modem, chi a diritto di fare qualunque cosa che, nell'esercizio delle proprie funzioni entri in relazione con il mondo esterno.

Tavola 19.: chi-fa-cosa fuori

Gruppi	Servizi	Diritti	Orari
Segretario Generale	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	Nessuno	Nessuna limitazione
Sviluppo Organizzativo e Politiche del Personale	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	Nessuno	Nessuna limitazione
Area Tecnica: Edilizia – Patrimonio - Suap	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	Nessuno	Nessuna limitazione
Area Tecnica: Servizio Lavori Pubblici	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	Nessuno	Nessuna limitazione
Area Tecnica: Pianificazione territoriale	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	Nessuno	Nessuna limitazione
Area Tecnica: Servizi Ambientali	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione



segue

Gruppi	Servizi	Diritti	Orari
	FTP	Nessuno	Nessuna limitazione
Area Tecnica: Commercio Servizio Amm.vi	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	Nessuno	Nessuna limitazione
Polizia Municipale	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	Nessuno	Nessuna limitazione
Area Servizi alla Persona e Comunicazione ed Istituzione Sister	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	Nessuno	Nessuna limitazione
Area Affari Generali: URP Segreteria e Ufficio Legale	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	Nessuno	Nessuna limitazione
Area Affari Generali: Servizi demografici	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	Nessuno	Nessuna limitazione
Sistemi Informativi	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	R/W	Nessuna limitazione
Area Bilancio: Servizio Bilancio	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione



segue

Gruppi	Servizi	Diritti	Orari
	FTP	Nessuno	Nessuna limitazione
Area Bilancio: U.O. Provveditorato – Economato	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	Nessuno	Nessuna limitazione
Area Controllo di Gestione e Tributi	Posta	R/W	Nessuna limitazione
	Navigazione	Nessuna limitazione	Nessuna limitazione
	FTP	Nessuno	Nessuna limitazione

Chi, interno, fa cosa da fuori

Oggetto dell'analisi è chi, membro dell'organizzazione, ha necessità di accedere dall'esterno alla rete dell'ente allo scopo di definire i diritti e per fare cosa.

Tavola 20.: chi, interno, fa-cosa da fuori

Gruppi	Persone	Diritti
Segretario Generale	Sindaco, Vice-Sindaco, Segretario	Nessuno
Sviluppo Organizzativo e Politiche del Personale	Nessuno	Nessuno
Area Tecnica: Edilizia – Patrimonio - Suap	Fabrizio Ruscelloni	Nessuno
Area Tecnica: Servizio Lavori Pubblici	Fabrizio Ruscelloni	Nessuno
Area Tecnica: Pianificazione territoriale	Fabrizio Ruscelloni	Nessuno
Area Tecnica: Servizi Ambientali	Fabrizio Ruscelloni - Carini Paolo	Gli stessi in LAN
Area Tecnica: Commercio Servizio Amm.vi	Fabrizio Ruscelloni	Nessuno



segue

Gruppi	Persone	Diritti
Polizia Municipale	Postazione mobile Vigili urbani Stefano Fabbri	Comandante
Area Servizi alla Persona e Comunicazione ed Istituzione Sister	Nessuno	Nessuno
Area Affari Generali: URP Segreteria e Ufficio Legale	Nessuno	Nessuno
Area Affari Generali: Servizi demografici	Nessuno	Nessuno
Sistemi Informativi	Capasso Francesco, Tinti Simone	Nessuno
Area Bilancio: Servizio Bilancio	Nessuno	Nessuno
Area Bilancio: U.O. Provveditorato – Economato	Nessuno	Nessuno
Area Controllo di Gestione e Tributi	Nessuno	Nessuno

Occorre ricordare che gli utenti eventualmente autorizzati entrano con gli stessi diritti di quando lavorano in LAN, ovvero dal proprio posto di lavoro interno.

Chi, esterno, può fare cosa da fuori o, in casi definiti, da dentro

Infine analizziamo chi esterno all'organizzazione, come un fornitore o un partner, può fare cosa nel momento in cui accede ai sistemi informativi interni all'organizzazione.

Tavola 21.: chi, esterno, può fare-cosa, da fuori o, in casi definiti, da dentro

Azienda	Server o apparecchiatura o servizio	Diritti	Orari
Cedaf	Server10	R/W Amministrazione	Client VPN nessuna limitazione
ADS	Server di contabilità	R/W Amministrazione	Client VPN nessuna limitazione
Softech	Server Garsia WE, Sosia e Gradus	R/W Amministrazione, ma con accesso presenziato	Nessuna limitazione
Apra	Server Tributi	R/W Amministrazione, ma con accesso presenziato	Nessuna limitazione
Solari	Server presenze/assenze	R/W	Solo con presenza fisica all'interno dell'ente
COOPERATIVA PICTOR Impresa di pulizie	Potenzialmente tutti i dati cartacei	nessuno	Orari previsti dal contratto
GAMBA SERVICE Impresa di pulizie	Potenzialmente tutti i dati cartacei	nessuno	Orari previsti dal contratto
Andraghetti Enzo	Archivio corrente e di deposito	Accesso solo ai documenti amministrativi per riordino pratiche cartacee	Orari previsti dal contratto



segue

Azienda	Server o apparecchiatura o servizio	Diritti	Orari
Fondazione ISFEL	Pratiche previdenziali/contributive	Accesso all'U.O. Sviluppo Organizzativo e Politiche del Personale solo con presenza fisica di altri dipendenti dell'U.O. per visione fascicoli del personale	Studio fascicoli del personale/Compilazione pratiche con propri programmi presso la propria sede
Lepida	Servizio Tetra – Polizia municipale, apparecchiature radio – r/w con accesso presenziato	r/w con accesso presenziato	Nessuna limitazione
EUROCOM	videosorveglianza	r/w con accesso presenziato	Nessuna limitazione
Carabinieri	Accesso all'anagrafe	R	Nessuna limitazione

Rapporti con aziende esterne all'organizzazione assimilabili a titolari del trattamento: regola 19.7 dell'Allegato B al Codice

Allo scopo di assicurare un servizio di manutenzione ordinaria gestito in outsourcing è necessario che alcune società esterne possano intervenire sui sistemi informativi dell'ente. Dette società prestano l'assistenza dovuta al fine di garantire la continuità del servizio, il ripristino dei sistemi in caso di fault, blocco o disastro.

Per l'elenco delle suddette società è possibile fare riferimento al piano di sicurezza dell'ente al paragrafo precedente dal titolo: *“Chi esterno fa cosa da fuori”*.

In questo paragrafo si intende, invece, sottolineare che i rapporti con queste strutture sono regolati da una apposita convenzione che le nomina “responsabili esterni all'organizzazione” ai sensi dell'art. 29 del d.lgs n. 196/2003.

Nella convenzione si fa presente che le società esterne che intervengono sul sistema informativo dell'ente avendo, di regola, diritti di amministratore, in teoria possono fare tutto. In ragione di ciò è imposto loro di intervenire solo con atti necessari alla prestazione dei servizi oggetto di contratto. E' fatto loro esplicito divieto di consultare, copiare, cancellare e fare qualunque operazione sui dati oggetto di trattamento, a meno di diversa autorizzazione scritta da parte del responsabile del trattamento dei dati. È fatto inoltre divieto, salvo diversa autorizzazione scritta da parte dell'amministratore dei sistemi, di cancellare i log riportanti *“chi ha fatto cosa”* sui dati.

Securelaw

Securelaw: verifica degli adempimenti formali

Dati residenti su elaboratori elettronici

Tavola 22.: riepilogo adempimenti formali per dati residenti su elaboratori elettronici

Adempimenti formali	Persona fisica o giuridica interessata	Modalità/conseguenze
Censimento delle banche dati.	Il gruppo di lavoro di progetto.	Espletata con il presente documento.
Notifica al garante		Non necessaria in quanto l'ente non gestisce alcun dato di quelli previsti all'art 37 comma 1 del D.lgs. 196/2003
Identificazione del titolare del trattamento dei dati.	Il Comune di Castenaso nella persona del legale rappresentante, Dott. Sermenghi	
Identificazione del/dei responsabili del trattamento dei dati (colui che è preposto al trattamento dei dati e che è soggetto alla vigilanza del titolare).	Nel corso del 2008 sono nominati responsabili tutti i dirigenti dell'Ente, con apposita lettera di incarico, ciascuno per i trattamenti e le banche dati di propria competenza	Nomina per iscritto riconfermata con il presente atto.
Amministratore di sistema (è il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione).	Tutti coloro che sono nominati nell'atto di incarico specifico che è stato redatto entro i termini previsti dal provvedimento del garante	Nominato per iscritto riconfermato con il presente atto.
Il custode delle chiavi - o password (persona fisica che opera in costante contatto con gli incaricati e che ha il	Non è previsto	



segue

Adempimenti formali	Persona fisica o giuridica interessata	Modalità/conseguenze
compito di custodire la password da essi stabilita ed annotata in busta chiusa conservata in armadio sotto chiave).		
Identificazione degli incaricati (persona fisica che provvede quotidianamente al trattamento).	Tutti gli utenti definiti nel presente documento.	È tenuto ad operare secondo le istruzioni e le direttive impartite in forma scritta dal titolare e dal responsabile.
Interessato (è la persona fisica o giuridica alla quale si riferiscono i dati)	Tutti coloro che vengono in contatto diretto con l'ente	Deve dare l'assenso al trattamento dei propri dati per iscritto

Securelaw: verifica degli adempimenti sostanziali

Occorre innanzitutto ribadire la regola generale che vige all'interno dell'ente per ciò che concerne i dati elettronici, che consiste nella comunicazione, avvenuta anche attraverso i corsi di formazione istituiti, a tutti gli incaricati del divieto di archiviare alcun tipo di dato sul proprio posto di lavoro/personal computer, pena l'acquisizione della piena responsabilità del trattamento di quei dati e le relative conseguenze civili e penali in capo all'incaricato/responsabile in caso di perdita e trafugamento dei dati medesimi.

Nel d.lgs. n. 196/2003 il legislatore richiede di adottare misure idonee volte a garantire la sicurezza e l'integrità dei dati: è opinione corrente della giurisprudenza che si debba intendere che tali misure siano scelte in relazione alle conoscenze acquisite in base al progresso tecnologico. Di conseguenza, per rispettare la normativa in vigore, è necessario aggiornarsi continuamente alle più recenti misure di protezione degli archivi di dati che siano rese disponibili dal produttore o dal mercato nel suo complesso.

Il d.lgs. n. 196/2003, Allegato B richiede di adottare misure minime che non si limitano alla protezione in senso tecnico dei sistemi informatici, ma si estendono: alla predisposizione di impianti antincendio che prevengano la distruzione di archivi, alla trasmissione degli stessi a società specializzate per l'archiviazione in armadi protetti, alla pianificazione di regole interne per la disciplina del comportamento degli incaricati (es. non attaccare memo di carta riportanti la password sul monitor del PC), ecc.

Si prende atto che l'ente dichiara di essere in linea con quanto previsto dalla normativa: di seguito si riepilogano le azioni poste in essere.

Adempimenti sostanziali dati elettronici

Tavola 23.: riepilogo adempimenti sostanziali per dati residenti su elaboratori elettronici

Adempimenti sostanziali	
a)	Password per l'accesso ai dati con dovere per l'utente di cambiarla.
b)	Sono stati nominati amministratori di sistema tutti coloro che sono stati indicati nell'atto di incarico specifico redatto entro i termini previsti dal provvedimento del garante
c)	Uno user-id per ogni incaricato, user-id che deve essere cancellato entro sei mesi dal termine dell'incarico.
d)	Programma antivirus sia lato server che lato personal computer che è aggiornato ogni volta che il produttore rilascia la disponibilità di un aggiornamento. Il prodotto adottato è dato dalla suite della Trend Micro, ovvero Office Scan per tutti i server e per tutti i client, nonché Panda sul perimetro (server di posta). Alcuni computer hanno in alternativa sistemi Avast
e)	Sistema di sicurezza che prevenga l'azione degli hackers (pirati informatici), anti intrusione e volto ad evitare accessi non autorizzati.
f)	Redazione del documento programmatico sulla sicurezza dei dati.
g)	È stato redatto un manuale contenente le istruzioni per gli incaricati che comprende: 1. L'elencazione specifica degli incaricati. 2. La descrizione del profilo assegnato nell'ambito dello svolgimento delle mansioni previste dall'incarico, con riferimento al trattamento dei dati personali. 3. L'elencazione dei dati a cui possono avere accesso e delle eventuali restrizioni (autorizzazione che deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento). 4. Il comportamento da assumere in caso di malfunzionamento del sistema (può anche essere semplicemente l'indicazione di richiedere l'intervento dell'assistenza tecnica). 5. Le istruzioni per l'utilizzo dei supporti magnetici. 6. Elenco ed ubicazione degli elaboratori abilitati alla connessione verso l'esterno. 7. Altre eventuali specifiche istruzioni.
h)	Almeno una volta all'anno il titolare, o se designato, il responsabile, devono verificare la correttezza di tali informazioni e, se necessario, provvedere alla loro modifica

Securelaw: verifica degli adempimenti formali

Dati residenti su archivi cartacei

Tavola 24.: riepilogo adempimenti formali per dati residenti su archivi cartacei

Adempimenti formali	Persona fisica o giuridica interessata	Modalità/conseguenze
Censimento delle banche dati.	Gruppo di lavoro di progetto	Espletata con il presente documento.
Notifica al garante		Non necessaria.
Identificazione del titolare del trattamento dei dati.	Il Comune di Castenaso nella persona del legale rappresentante, Dott. Sermenghi	
Identificazione del/dei responsabili del trattamento dei dati (colui che è preposto al trattamento dei dati e che è soggetto alla vigilanza del titolare).	Nel corso del 2008 sono nominati responsabili tutti i dirigenti dell'Ente, con apposita lettera di incarico, ciascuno per i trattamenti e le banche dati di propria competenza	Nomina per iscritto riconfermata con il presente atto.
Identificazione degli incaricati (persona fisica che provvede quotidianamente al trattamento).	Tutti gli utenti definiti nel presente documento.	È tenuto ad operare secondo le istruzioni e le direttive impartite in forma scritta dal titolare e dal responsabile.
Interessato (è la persona fisica o giuridica alla quale si riferiscono i dati)	Tutti coloro che vengono in contatto diretto con l'ente	Deve dare l'assenso al trattamento dei propri dati per iscritto

Adempimenti sostanziali dati cartacei

Tavola 25.: riepilogo adempimenti sostanziali per dati residenti su archivi cartacei

Adempimenti sostanziali	
a)	È stato redatto un manuale contenente le istruzioni per gli incaricati che comprende: 1. L’elencazione specifica degli incaricati. 2. Il piano di formazione annuale degli incaricati. 3. L’identificazione del gruppo di appartenenza ai fini del trattamento dei dati personali. 4. L’elencazione dei dati a cui gli incaricati possono avere accesso e delle eventuali restrizioni (autorizzazione che deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento). 5. Il comportamento da assumere in caso di necessità di distruzione di documenti erroneamente stampati. 6. Altre eventuali specifiche istruzioni.
b)	Definizione dei rapporti con i soggetti esterni che si configurano come responsabili del trattamento dei dati.
c)	Almeno una volta all’anno il titolare, o se designato, il responsabile, devono verificare la correttezza di tali informazioni e, se necessario, provvedere alla loro modifica.

Securelaw: piano formativo degli incaricati: regola 19.6 dell'Allegato B al Codice

In ottemperanza all'Allegato B del "Codice in materia di protezione dei dati" sono previsti *interventi formativi degli incaricati del trattamento per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare*. La formazione è prevista a partire dal primo ingresso nell'ente e procede per l'intera vita lavorativa, divenendo particolarmente significativa in occasioni di mutamenti di mansione e di introduzione di nuovi significativi strumenti ai fini del trattamento dei dati.

Può non essere superfluo ricordare che un mirato e programmato processo di formazione favorisce una condivisione di regole e valori che permettono all'ente di operare in condizioni di efficacia ed efficienza.

Il piano di formazione degli incaricati può riguardare tre diverse tipologie di utenti:

- Utenti in pianta organica.
- Neoassunti.
- Utenti in revisione di incarico.

Utenti in pianta organica.

Per questa prima tipologia di utenti sono previsti due livelli di attività formativa:

1. una sessione iniziale volta a far apprendere le seguenti conoscenze:
 - lo spirito e i contenuti della legge;
 - le istruzioni impartite nel manuale degli incaricati;
 - le informazioni specifiche inerenti il trinomio incarico/profilo/unità-organizzativa o gruppo.
2. una sessione periodica di aggiornamento volta a spiegare:
 - le eventuali novità di legge;
 - le novità tecnologiche introdotte volte ad aumentare il livello di sicurezza secondo lo spirito di "adeguamento tecnologico" suggerito dalla normativa.

Utenti neoassunti.

Per questa seconda tipologia di utenti sono previsti due livelli di attività formativa:



segue

1. una sessione iniziale prevista all'interno del percorso formativo del dipendente e da tenersi sotto la responsabilità del dirigente di settore al quale afferisce il neoincaricato volta a far apprendere:
 - lo spirito e i contenuti della legge;
 - le istruzioni impartite nel manuale degli incaricati;
 - le informazioni specifiche inerenti il trinomio incarico/profilo/unità-organizzativa o gruppo.
2. la partecipazione alle sessioni periodiche di aggiornamento (come sopra indicato).

Utenti in revisione di incarico

Per questa ultima tipologia di utenti sono previsti due livelli di attività formativa:

1. una sessione iniziale prevista all'interno del percorso formativo del dipendente e da tenersi sotto la responsabilità del dirigente di settore al quale afferisce il neoincaricato volta a far apprendere:
 - le differenze nella gestione dei dati relative al nuovo incarico, rispetto al precedente;
 - istruzioni impartite nel manuale degli incaricati.
2. la partecipazione alle sessioni periodiche di aggiornamento (come sopra indicato).

Le modalità di erogazione dell'attività formativa possono avvenire attraverso lezioni frontali o dialogate in aula, nonché attraverso le più moderne tecnologie di e-learning. Nel caso si scegliesse quest'ultima modalità, si consiglia di prevedere una fase di verifica dell'apprendimento delle conoscenze e competenze oggetto del percorso formativo.

Tavola 26.: piano di formazione degli utenti

Corso di formazione	Descrizione sintetica	Classi di incarico interessate	Numero di incaricati interessati	Numero di incaricati già formati/ da formare nell'anno	Calendario
Il nuovo Codice sulla Tutela dei dati personali ed il manuale utente	Riassunto legislativo e spiegazione del manuale degli incaricati in aula per i dirigenti ed in e-learning per gli incaricati	Segreteria Generale	Tutti	Tutti	Tenuti nel mese di novembre 2006
Il nuovo Codice sulla Tutela dei dati personali ed il manuale utente	Riassunto legislativo e spiegazione del manuale degli incaricati in aula per i dirigenti ed in e-learning per gli incaricati	Sviluppo Organizzativo e Politiche del Personale	Tutti	Tutti	Tenuti nel mese di novembre 2006
Il nuovo Codice sulla Tutela dei dati personali ed il manuale utente	Riassunto legislativo e spiegazione del manuale degli incaricati in aula per i dirigenti ed in e-learning per gli incaricati	Area Tecnica: Edilizia – Patrimonio - Suap	Tutti	Tutti	Tenuti nel mese di novembre 2006
Il nuovo Codice sulla Tutela dei dati personali ed il manuale utente	Riassunto legislativo e spiegazione del manuale degli incaricati in aula per i dirigenti ed in e-learning per gli incaricati	Area Tecnica: Servizio Lavori Pubblici	Tutti	Tutti	Tenuti nel mese di novembre 2006

Il nuovo Codice sulla Tutela dei dati personali ed il manuale utente	Riassunto legislativo e spiegazione del manuale degli incaricati in aula per i dirigenti ed in e-learning per gli incaricati	Area Tecnica: Pianificazione territoriale	Tutti	Tutti	Tenuti nel mese di novembre 2006
Il nuovo Codice sulla Tutela dei dati personali ed il manuale utente	Riassunto legislativo e spiegazione del manuale degli incaricati in aula per i dirigenti ed in e-learning per gli incaricati	Area Tecnica: Servizi Ambientali	Tutti	Tutti	Tenuti nel mese di novembre 2006
Il nuovo Codice sulla Tutela dei dati personali ed il manuale utente	Riassunto legislativo e spiegazione del manuale degli incaricati in aula per i dirigenti ed in e-learning per gli incaricati	Area Tecnica: Commercio Servizi Amm.vi	Tutti	Tutti	Tenuti nel mese di novembre 2006
Il nuovo Codice sulla Tutela dei dati personali ed il manuale utente	Riassunto legislativo e spiegazione del manuale degli incaricati in aula per i dirigenti ed in e-learning per gli incaricati	Polizia Municipale	Tutti	Tutti	Tenuti nel mese di novembre 2006
Il nuovo Codice sulla Tutela dei dati personali ed il manuale utente	Riassunto legislativo e spiegazione del manuale degli incaricati in aula per i dirigenti ed in e-learning per gli incaricati	Area Servizi alla Persona e Comunicazione ed Istituzione Sister	Tutti	Tutti	Tenuti nel mese di novembre 2006

Il nuovo Codice sulla Tutela dei dati personali ed il manuale utente	Riassunto legislativo e spiegazione del manuale degli incaricati in aula per i dirigenti ed in e-learning per gli incaricati	Area Affari Generali: URP Segreteria e Ufficio Legale	Tutti	Tutti	Tenuti nel mese di novembre 2006
Il nuovo Codice sulla Tutela dei dati personali ed il manuale utente	Riassunto legislativo e spiegazione del manuale degli incaricati in aula per i dirigenti ed in e-learning per gli incaricati	Area Affari Generali: Servizi demografici	Tutti	Tutti	Tenuti nel mese di novembre 2006
Il nuovo Codice sulla Tutela dei dati personali ed il manuale utente	Riassunto legislativo e spiegazione del manuale degli incaricati in aula per i dirigenti ed in e-learning per gli incaricati	Sistemi Informativi	Tutti	Tutti	Tenuti nel mese di novembre 2006
Il nuovo Codice sulla Tutela dei dati personali ed il manuale utente	Riassunto legislativo e spiegazione del manuale degli incaricati in aula per i dirigenti ed in e-learning per gli incaricati	Area Bilancio: Servizio Bilancio	Tutti	Tutti	Tenuti nel mese di novembre 2006
Il nuovo Codice sulla Tutela dei dati personali ed il manuale utente	Riassunto legislativo e spiegazione del manuale degli incaricati in aula per i dirigenti ed in e-learning per gli incaricati	Area Bilancio: U.O. Provveditorato – Economato	Tutti	Tutti	Tenuti nel mese di novembre 2006



segue

Il nuovo Codice sulla Tutela dei dati personali ed il manuale utente	Riassunto legislativo e spiegazione del manuale degli incaricati in aula per i dirigenti ed in e-learning per gli incaricati	Area Controllo di Gestione e Tributi	Tutti	Tutti	Tenuti nel mese di novembre 2006
--	--	--------------------------------------	-------	-------	----------------------------------

Data di aggiornamento: 14/03/2010

DPS Documento Programmatico sulla Sicurezza dei dati: le azioni

Dati residenti su supporto cartaceo

Analisi dei rischi

I rischi ai quali sono soggetti i dati residenti su supporto cartaceo presenti nell'ente sono molto minori, ma comunque possiamo così elencarli:

- Accesso indebito alle risorse sia da parte di personale interno non autorizzato.
- Rischi connessi alla trasmissione dei dati.
- Perdita dei dati e quindi perdita della loro integrità fisica.
- Furto e azioni dolose.
- Eventi dannosi o disastrosi.
- Rischi connessi alla procedura di eliminazione di dati erroneamente stampati.

Analisi dei rischi e delle azioni intraprese per cautela relativamente al trattamento dei dati cartacei: regola 19.4 dell'Allegato B al Codice

Le soluzioni individuate per la protezione dei dati residenti su elaboratori sono diverse e sono di seguito elencate.

Tavola 27.: riepilogo dei rischi e delle azioni legate al trattamento dei dati cartacei

Rischio	Azione
Criteri e procedure per evitare <u>l'accesso indebito alle risorse da parte di utenti interni</u> all'ente	• Ogni utente autorizzato ha le chiavi dell'ente o degli uffici di propria pertinenza (si veda tabella relativa). È fatto divieto assoluto agli incaricati di recarsi in locali per i quali l'accesso non è autorizzato.
Criteri e procedure per disciplinare il <u>comportamenti degli operatori</u>	• Formazione periodica di tutti gli incaricati • Controlli periodici circa l'operato degli utenti • Controlli degli accessi, sia fisici che informatici

Rischio	Azione
Criteri e procedure per disciplinare gli <u>eventi relativi al contesto</u>	Tutti i locali sono ad accesso controllato
Criteri e procedure per assicurare la <u>sicurezza nelle trasmissioni</u> dei dati	I dati su supporto cartaceo sono consegnati solo a corriere postale o ad un corriere privato o ad altro operatore autorizzato
Criteri e procedure per assicurare l' <u>integrità fisica</u> dei dati	Tutti i locali sono protetti da un sistema antincendio a norma 626.
Criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché individuazione delle procedure per controllare l'accesso delle persone autorizzate ai locali medesimi: ciò al fine di evitare al massimo <u>manomissioni o furti o azioni dolose</u>	Ogni utente autorizzato ha le chiavi dell'ente o degli uffici di propria pertinenza (si veda tabella relativa). È fatto divieto assoluto agli incaricati di recarsi in locali per i quali l'accesso non è autorizzato.
<u>Eventi dannosi o disastrosi</u>	- Tutti i dati su supporto cartaceo prodotti dall'ente possono comunque riprodotti in ogni momento partendo dagli archivi elettronici. - I dati ricevuti in futuro saranno oggetto di digitalizzazione
<u>Rischi connessi alla procedura di eliminazione di dati erroneamente stampati.</u>	Tutti i supporti cartacei che devono essere distrutti finiscono in alcuni raccoglitori solo dopo essere stati stracciati
Elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni	Ogni volta che si presenta la necessità vengono tenute delle sessioni di aggiornamento, anche nell'ambito della formazione all'utilizzo dei nuovi strumenti informatici, volte ad assicurare tale conoscenza e l'aggiornamento della stessa
Controlli periodici	Il responsabile effettua controlli periodici annuali circa l'applicazione delle regole suddette



segue

Dati residenti su elaboratori elettronici

Analisi dei rischi

Come evidenziato sopra, i rischi ai quali sono soggetti i dati residenti sugli elaboratori presenti nell'ente, già precedentemente elencati, sono i seguenti:

- Accesso indebito alle risorse sia da parte di personale interno non autorizzato, che da parte di "pirati" esterni
- Rischi connessi alla trasmissione dei dati
- Perdita dei dati e quindi perdita della loro integrità fisica
- Errori operativi volti a minare l'integrità logica dei dati
- Azioni dolose
- Manomissioni o furti
- Eventi dannosi o disastrosi

Analisi dei rischi e delle azioni intraprese per cautela: regola 19.4 dell'Allegato B al Codice

Le soluzioni individuate per la protezione dei dati residenti su elaboratori sono diverse e sono di seguito elencate.

Tavola 28.: analisi dei rischi e azioni intraprese per i dati residenti su supporto elettronico

Rischio	Azione
Criteri e procedure per evitare <u>l'accesso indebito alle risorse da parte di utenti interni</u> all'ente	• Ogni utente ha un codice identificativo ed una password che lo abilitano ad entrare nel sistema di rete limitatamente ai dati necessari per lo svolgimento delle proprie mansioni. La password è a scadenza secondo i requisiti normativi • Ogni utente ha un codice identificativo ed una password che lo abilitano ad entrare nel sistema applicativo limitatamente ai dati necessari per lo svolgimento delle proprie mansioni. La password è a scadenza, ove possibile, secondo i requisiti normativi
Criteri e procedure per disciplinare il <u>comportamenti degli</u>	• Formazione periodica di tutti gli incaricati



segue

Rischio	Azione
<u>operatori</u>	• Controlli periodici circa l'operato degli utenti • Controlli degli accessi, sia fisici che informatici
Criteri e procedure per disciplinare gli <u>eventi relativi agli strumenti</u>	• Aggiornamento e potenziamento periodico dei sistemi antivirus installati • Azioni specifiche previste per il fault tolerance (vedi tabelle successive)
Criteri e procedure per disciplinare gli <u>eventi relativi al contesto</u>	• Tutti i locali sono ad accesso controllato • I sistemi di condizionamento del CED sono a tolleranza di guasto, ed in caso di guasto è pronta ad intervenire la società che ne ha in gestione la manutenzione
Criteri e procedure per assicurare la <u>sicurezza nelle trasmissioni</u> dei dati	• L'accesso alla rete pubblica degli utenti è regolamentato da strumenti tecnici (firewall) che consentono l'accesso al servizio solo agli incaricati che ne hanno necessità e registrano le attività fatte • I suddetti sistemi proteggono la rete locale da accessi indebiti alle risorse da parte di "pirati" esterni • La comunicazione con alcuni fornitori avviene attraverso VPN • È fissato un piano di controllo settimanale le cui responsabilità ed oneri sono descritti nella tabella di cui sotto
Criteri e procedure per assicurare <u>l'integrità fisica</u> dei dati	• Servizi di back-up le cui responsabilità ed oneri sono descritti nella tabella di cui sotto • I nastri di back-up sono normalmente archiviati in cassaforte presente all'interno della sede del Municipio. • Gli altri strumenti di back-up delle sedi remote e



segue

Rischio	Azione
	non collegate, sono archiviati, sotto chiave, nelle singole sedi • È installato un sistema antivirus. Il prodotto adottato è dato dalla suite della Trend Micro, Office Scan per tutti i server e per tutti i client, nonché Panda sul perimetro. Alcuni computer hanno in alternativa sistemi Avast
Criteri e procedure per assicurare <u>l'integrità logica</u> dei dati	• Le applicazioni software in uso coprono l'ente da tale rischio
Criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché individuazione delle procedure per controllare l'accesso delle persone autorizzate ai locali medesimi: ciò al fine di evitare al massimo <u>manomissioni o furti o azioni dolose</u>	• I server di rete sono localizzati in un ambiente CED ad accesso controllato, la cui chiave è nelle mani esclusive dei membri del Servizio Informatico e delle altre persone autorizzate • I locali del CED sono protetti da un sistema antifurto
Criteri tecnici ed organizzativi per limitare al massimo gli effetti di <u>eventi dannosi o disastrosi</u>	• I dati tutti i giorni sono replicati su un device (NAS) a San Lazzaro presso il CED del SIA
Elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni	• Ogni volta che si presenta la necessità vengono tenute delle sessioni di aggiornamento, anche nell'ambito della formazione all'utilizzo dei nuovi strumenti informatici, volte ad assicurare tale conoscenza e l'aggiornamento della stessa
Controlli periodici	• Il responsabile e l'amministratore di sistema effettuano controlli periodici annuali circa l'applicazione delle regole suddette

Descriviamo ora di seguito in modo dettagliato le attività più importanti intraprese per affrontare i rischi sopra riportati

Le operazioni di salvataggio dei dati: regola 19.5 dell'Allegato B al Codice

Si presenta, di seguito, il piano di sicurezza specifico per le operazioni di salvataggio dei dati, che nell'ambito del D.p.s. è sicuramente il documento che riveste la maggiore importanza.

Il sistema di back-up dei dati dei server è separato per ogni server e centralizzato nelle responsabilità: è fatto su dischi esterni e successivamente riversato su nastro.

Il ciclo delle cassette è di 6 giorni.

Non viene previsto alcun sistema di back-up dei client in quanto si è già specificato che tutti i dati sono e devono risiedere su server.

Di seguito elencheremo le operazioni previste, che fungono da manuale di istruzioni per gli incaricati addetti, ed il responsabile della esecuzione di tali operazioni.

Tavola 29.: riepilogo delle operazioni di salvataggio dei dati

1. eseguire giornalmente il back-up dei dati (Francesco Capasso)
2. archiviare i nastri dei back-up sotto chiave (Francesco Capasso)
3. controllare che le versioni del software di back-up siano allineate alle ultime versioni disponibili (Francesco Capasso)
4. eseguire trimestralmente una prova di restore parziale dei dati (Francesco Capasso)
5. eseguire settimanalmente un back-up intero dei dati (Francesco Capasso)
6. archiviare provvedere a centralizzare in luogo definito, CD ROM dei sistemi operativi e dei software di sistema, in modo da averli sempre a disposizione in caso di bisogno (Francesco Capasso)
7. provvedere a centralizzare in luogo definito e sicuro, copie dei back-up (cassaforte), in modo da averli sempre a disposizione in caso di bisogno (Francesco Capasso)

I controlli anti-intrusione dall'esterno

Presentiamo di seguito il piano di sicurezza relativo ai controlli anti-intrusione: anche in questo caso elencheremo le operazioni previste, che fungono da manuale di istruzioni per gli incaricati addetti, ed il responsabile della esecuzione di tali operazioni.

Il controllo degli attacchi viene fatto attraverso il prodotto Snort.

Tavola 30.: riepilogo delle operazioni di controlli anti-intrusione dall'esterno

1. tenere aperto il monitor relativo ai tentativi di intrusione che il firewall offre (Francesco Capasso)
2. eseguire giornalmente il controllo del log relativo ai tentativi di intrusione (Francesco Capasso)
3. avvisare il responsabile sistemi informativi dei dati di eventuali attacchi (Francesco Capasso)
4. attivare azioni correttive (Francesco Capasso)
5. chiedere consulenza al fornitore dell'assistenza sistemistica su altre precauzioni da adottare (Francesco Capasso)

Azioni intraprese per il fault tolerance: regola 19.5 dell'Allegato B al Codice

Le soluzioni adottate per attivare un meccanismo di fault tolerance per ciascuno dei device in elenco sono strettamente legate al fattore criticità ed al tipo di device di fronte al quale ci troviamo. Come si evince dall'elenco ci troviamo di fronte ai seguenti sistemi che possiamo così catalogare:

Server Windows NT/2000

Server Linux

Server di data base SQL Server

Switch

Router di fascia alta

Router di fascia bassa

Linee telefoniche o in fibra di collegamento con le sedi remote

Analizziamo ora le azioni adottate per ciascun elemento

Server Windows NT/200X

Per questo tipo di server il fattore di criticità varia dal livello 2 al livello 4. Anche in questo caso le soluzioni adottate sono diverse. Vediamole una per una.

Server 200X/NT in categoria 4

In questa categoria abbiamo alcuni server. I servizi su questi server sono critici, ma esistono già dei sistemi di fault tolerance sui dischi (Raid5); e sulle memorie RAM. Come per tutti i server, la macchina è coperta da 3 anni di garanzia e dopo il terzo anno è previsto il servizio indicato nel contratto di manutenzione. Le operazioni sopra riportate sono eseguite dal responsabile della rete interna (Francesco Capasso). In caso di assenza del responsabile di rete l'operazione può essere fatta da uno qualunque dei membri del Servizio Informatico

I servizi di PDC sono coperti a caldo da quelli del server BDC

DB Server

Per detto server il fattore criticità è sempre a livello 4, in quanto senza tale server gli utenti non possono lavorare sulle applicazioni gestionali ed accedere ai propri archivi. I servizi su questi server sono critici, ma esistono già dei sistemi di



segue

fault tolerance sui dischi (Raid5). Per quello che riguarda il server DB Server, passato il periodo di garanzia, è stabilito un contratto con la Idem che garantisce, a fronte di una chiamata, tempi di intervento di 4 ore per ripristinare le funzionalità del server stesso. Le operazioni sopra riportate sono eseguite dal responsabile della rete interna (Francesco Capasso). In caso di assenza del responsabile di rete l'operazione può essere fatta da uno qualunque dei membri del Servizio Informatico.

Server 200X in categoria 3 e 2

In questa categoria abbiamo il server Domino e numerosi server di applicazioni minori. I servizi su questi server sono decisamente meno critici, ma esistono comunque sistemi di fault tolerance sui dischi, mentre le memorie RAM attive sono a correzione di errore. Come per tutti i server, la macchina è coperta da 3 anni di garanzia e dopo il terzo anno è previsto il servizio indicato nel contratto di manutenzione. Le operazioni sopra riportate sono eseguite dal responsabile della rete interna (Francesco Capasso). In caso di assenza del responsabile di rete l'operazione può essere fatta da uno qualunque dei membri del Servizio Informatico.

Server Virtuali

Per tali server il fattore criticità è sempre a livello 4, in quanto senza tali server gli utenti non possono lavorare sulle applicazioni gestionali ed accedere ai propri archivi. I servizi su questi server sono critici, ma esistono già dei sistemi di fault tolerance sui dischi (Raid5). Per quello che riguarda i server, passato il periodo di garanzia, è stabilito un contratto con la IDEM che garantisce, a fronte di una chiamata, tempi di intervento di 4 ore per ripristinare le funzionalità del server stesso. Le operazioni sopra riportate sono eseguite dal responsabile della rete interna. In caso di assenza del responsabile di rete l'operazione può essere fatta da uno qualunque dei membri del Servizio Informatico.

Server Linux

Per questo tipo di server il fattore di criticità varia dal livello 2 al livello 4. Anche in questo caso le soluzioni adottate sono diverse. Vediamole una per una.

Server Linux in categoria 4

In questa categoria abbiamo diversi server che hanno funzioni specifiche (tra cui anche quelle relative alla sicurezza). I servizi su questi server sono critici, ma esistono già dei sistemi di fault tolerance sui dischi (Raid1); e sulle memorie RAM. Il server è inoltre coperto da 3 anni di estensione garanzia.

Server Linux in categoria 2

In questa categoria abbiamo alcuni server. I servizi su questo server sono decisamente meno critici, ma esistono comunque sistemi di fault tolerance sui dischi, mentre le memorie RAM attive sono a correzione di errore. Come per tutti i server, la macchina è coperta da 3 anni di garanzia e dopo il terzo anno è previsto il servizio indicato nel contratto di manutenzione. Le operazioni sopra riportate sono eseguite dal responsabile della rete interna (Francesco Capasso). In



segue

caso di assenza del responsabile di rete l'operazione può essere fatta da uno qualunque dei membri del Servizio Informatico.

Server ESXi

Per questo tipo di server il fattore di criticità varia dal livello 2 al livello 4. Anche in questo caso le soluzioni adottate sono diverse. Vediamole una per una.

Server ESXi in categoria 4

I servizi su questi server sono critici, ma esistono già dei sistemi di fault tolerance sui dischi (Raid5); e sulle memorie RAM. Come per tutti i server, la macchina è coperta da 3 anni di garanzia e dopo il terzo anno è previsto il servizio indicato nel contratto di manutenzione. Le operazioni sopra riportate sono eseguite dal responsabile della rete interna (Francesco Capasso). In caso di assenza del responsabile di rete l'operazione può essere fatta da uno qualunque dei membri del Servizio Informatico

Server ESXi in categoria 2 e 3

In questa categoria abbiamo il server Domino e numerosi server di applicazioni minori. I servizi su questi server sono decisamente meno critici, ma esistono comunque sistemi di fault tolerance sui dischi, mentre le memorie RAM attive sono a correzione di errore. Come per tutti i server, la macchina è coperta da 3 anni di garanzia e dopo il terzo anno è previsto il servizio indicato nel contratto di manutenzione. Le operazioni sopra riportate sono eseguite dal responsabile della rete interna (Francesco Capasso). In caso di assenza del responsabile di rete l'operazione può essere fatta da uno qualunque dei membri del Servizio Informatico.

Switch

Attualmente nel Comune di Castenaso risultano installati diversi switch sui quali si basano tutta l'architettura di rete delle sedi interessate dal progetto ed hanno chiaramente un fattore di criticità che variano dal livello 4 al livello 3.

In caso di fault gli switch possono essere sostituiti, temporaneamente e con l'obiettivo di far ripartire un servizio, anche se ridotto, da un vecchio modello, disponibile a magazzino, oppure da un hub di scorta. La rete ripartirà comunque anche se con velocità ridotte. Le operazioni sopra riportate sono eseguite dal responsabile della rete interna (Francesco Capasso). In caso di assenza del responsabile di rete l'operazione può essere fatta da uno qualunque dei membri del Servizio Informatico.

Firewall e Router

I router sono classificati in fascia 4 in quanto costituiscono la portante delle comunicazioni dell'ente verso il mondo esterno. I router sono apparecchiature sulle quali non è sempre possibile prevedere un back-up a caldo e d'altronde non è possibile pensare di tenere una macchina di questo tipo di scorta in magazzino. Le precauzioni intraprese sono due:



segue

1. Il router che connette l'ente ad Internet tramite la rete a Larga Banda LEPIDA è in gestione e manutenzione ad Acantho.
2. Le connessioni in fibra ottica sono gestite tramite switch e apparecchiature relative (media converter, ecc.).
3. Il firewall è assistito direttamente in gestione e manutenzione dal Sistema Informativo Interno
4. Le connessioni XDSL e ISDN sono invece in assistenza Telecomitalia che garantisce tempi di intervento entro le 8 ore lavorative

Procedure da seguire in caso di fault

La procedura da seguire, che cercheremo di definire passo a passo, è strettamente legata alle soluzioni tecniche adottate. Vero è che quasi tutti i sistemi di fault tolerance individuati si attivano in modo automatico. Ci sono però delle azioni da eseguire comunque.

Server

Interventi validi per tutti i server installati

Fault di disco

Diversi i server sono al livello 4 della scala di criticità: tutti i server sono quindi coperti da un servizio di fault tolerance sui dischi che è in grado di intervenire senza operatore. In caso di rottura di un disco quindi gli utenti non subiranno interruzioni di lavoro, ed il responsabile del CED dell'ente si attiverà per aprire una chiamata al centro di assistenza hardware del modello interessato (qualora il server sia ancora in garanzia o sotto contratto di manutenzione), il quale interverrà per sostituire il disco. È opportuno controllare i tempi di intervento dell'assistenza. Contemporaneamente è necessario attivare il servizio interno di assistenza per affrontare eventuali operazioni di riconfigurazione che si dovessero eventualmente rendere necessarie.

Altro tipo di fault

Il responsabile del CED dell'ente si attiverà per aprire una chiamata al centro di assistenza hardware del modello interessato (qualora il server sia ancora in garanzia o sotto contratto di manutenzione), il quale interverrà per sostituire il pezzo difettoso. È opportuno controllare i tempi di intervento dell'assistenza. Contemporaneamente è necessario attivare il servizio interno di assistenza per affrontare eventuali operazioni di riconfigurazione che si dovessero eventualmente rendere necessarie.

Server Windows 200X

Tutti questi server reggono i più importanti servizi applicativi dell'ente. Le macchine quindi devono funzionare sempre. In caso di fault di un server le operazioni che il responsabile del CED dell'ente devono fare sono tre:

1. aprire immediatamente una chiamata al centro di assistenza del produttore hardware per segnalare il guasto;
2. aprire immediatamente una chiamata alla società che offre assistenza sistemistica per segnalare il problema e ricevere il supporto necessario;

**Il numero dell'assistenza tecnica da contattare in caso di bisogno è:
Il venditore della macchina per i primi 3 anni di garanzia**

Idem per le macchine fuori garanzia 051/760702

ADS 051/ 6307411

Successivamente alla riparazione sarà necessario:

3. riconfigurare il server danneggiato;

Server Linux

Tutti questi server reggono i più importanti servizi applicativi dell'ente. Le macchine quindi devono funzionare sempre. In caso di fault di un server le operazioni che il responsabile del CED dell'ente devono fare sono tre:

1. aprire immediatamente una chiamata al centro di assistenza per segnalare il guasto;
2. aprire immediatamente una chiamata alla società che offre assistenza sistemistica per segnalare il problema e ricevere il supporto necessario;

Il numero dell'assistenza tecnica da contattare in caso di bisogno è:

Il venditore della macchina per i primi 3 anni di garanzia

Idem per le macchine fuori garanzia 051/760702

Successivamente alla riparazione sarà necessario:

3. riconfigurare il server danneggiato;

Server Windows 200X – SQL Server

Questi server regge un servizio applicativo che tra i più importanti dell'ente. Le macchine quindi devono funzionare con regolarità. In caso di fault di un server le operazioni che il responsabile del CED dell'ente devono fare sono tre:

1. aprire immediatamente una chiamata al centro di assistenza di Cedaf per segnalare il guasto;
2. aprire immediatamente una chiamata alla società che offre assistenza sistemistica per segnalare il problema e ricevere il supporto necessario;

Il numero dell'assistenza tecnica da contattare in caso di bisogno è

Cedaf 0543/727011

Il venditore della macchina per i primi 3 anni di garanzia

Idem per le macchine fuori garanzia 051/760702

Successivamente alla riparazione sarà necessario:

3. riconfigurare il server danneggiato;



segue

Switch

Tutti gli switch garantiscono il lavoro di tutti gli utenti e quindi devono funzionare sempre. In caso di fault di uno switch le operazioni che il responsabile del CED dell'ente devono fare sono due:

1. accedere immediatamente al magazzino e recuperare uno switch o un hub di scorta;
2. provvedere alla sostituzione dello switch danneggiato con uno di scorta: gli utenti potranno così ricominciare a lavorare anche se con prestazioni ridotte;
3. aprire immediatamente una chiamata alla società che offre assistenza sistemistica per segnalare il problema e ricevere il supporto necessario;

Connessione ad Internet

I router di fascia alta installati sono tutti al livello 3 della scala di criticità: è chiaro che, essendo il cuore di tutta la comunicazione, devono essere soggetti al minimo numero di interruzioni possibili.

In caso di fault di detti router o firewall l'operazione che il responsabile di rete dell'ente deve fare è:

1. aprire immediatamente una chiamata presso la il sistema informativo interno o presso ACANTHO la quale provvederà gestire il guasto (che potrebbe essere anche sulla linea dati in fibra ottica) entro le ore fissate dal contratto ed a riconfigurare il servizio.

Il numero dell'assistenza tecnica da contattare in caso di bisogno è

Acantho Numero Verde Servizio Clienti: 800-055800

Router e connessioni WAN

Al momento non esistono router di fascia alta installati ma già qui prevediamo che si possano attivare tali collegamenti: è chiaro che, essendo il cuore di tutta la WAN, devono essere soggetti al minimo numero di interruzioni possibili

In caso di fault di detti router l'operazione che il responsabile di rete dell'ente deve fare è:

1. aprire immediatamente una chiamata presso il fornitore del router la quale provvederà gestire il guasto (che potrebbe essere anche sulla linea telefonica ADSL) entro le ore fissate dal contratto ed a riconfigurare il servizio;

Il numero dell'assistenza tecnica da contattare in caso di bisogno è

Da definire se e quando verranno attivati

2. aprire immediatamente una chiamata presso il centro di supporto Telecomitalia, per le connessioni



segue

XDSL/ISDN, il quale provvederà risolvere il problema entro le ore fissate dal contratto;

Il numero dell'assistenza tecnica da contattare in caso di bisogno è

Telecomitalia 191

Linee di collegamento in fibra ottica

Le linee di connessione installate fra le varie sedi dell'ente sono tutte al livello 4 della scala di criticità. In caso di indisponibilità di dette linee le operazioni che il responsabile di rete deve fare sono due:

1. aprire immediatamente una chiamata presso il centro di supporto Seit o LGM, per le linee in fibra ottica, il quale provvederà risolvere il problema entro le ore fissate dal contratto;

Il numero dell'assistenza tecnica da contattare in caso di bisogno è

LGM 051/ 6311743

Seit 051/6311801 - 0522/273711

Azioni da intraprendere per il disaster recovery

Dobbiamo innanzi tutto definire quali sono le sedi interessate allo studio di disaster recovery. Stabiliamo dunque che le sedi in oggetto sono due e sono costituite dalla sede principale dell'ente e dalla sede di disaster che è individuata presso gli Ufficio della Polizia Municipale. Chiameremo dunque A la sede principale e B la sede di di disaster.

A: Sede principale Piazza Bassi, n.1 40017 Castenaso (BO)

B: Sede di disaster recovery: c/o sede Polizia Municipale via Nasica 9 - Cap 40055 Castenaso (Bo)

C: Sede di archiviazione dei dati c/o Comune di San Lazzaro di Savana, Piazza Bracci , 1 40068 S. Lazzaro di Savena (Bo)

Regole valide per tutti i Server

Per i server i discorsi sono molteplici

1. Innanzi abbiamo definito ed attivato una procedura che permette di avere periodicamente i dati ricoverati in un luogo sicuro, nel nostro caso la sede di “archiviazione dei dati di back-up-disaster. Nel nostro caso dunque ogni giorno una copia incrementale dei back-up definita “disaster copy” viene effettuata dalla sede A alla sede di archiviazione dei dati C, pronta per essere trasferita nella sede B in caso di disastro.
2. In secondo luogo si ricorda che giornalmente si eseguono e si controllano i back-up ordinari

Server in categoria 2

1. Per i server basati su sistema operativo di tipo Windows NT/200X o Linux sono disponibili, secondo le modalità sopra indicate, i nastri di salvataggio, dai quali è possibile ricostruire i dati e le configurazioni dei server e la copia remota dei dati dell'ente.
2. Per poter fare in modo che questa cautela produca, in caso di bisogno, i suoi effetti, abbiamo previsto la disponibilità di un server “disaster” da installare presso la sede B, pronto per accogliere la restore dei dati: detto server verrà fornito, sulla base dell'accordo che il cliente ci ha detto di avere in essere con specifico fornitore, entro 3 giorni dalla richiesta nella sede B di disaster, completo di lettore dei nastri di back-up.

Server in categoria 1

1. Anche in questo caso per ogni sistema operativo presente di tipo Windows 200X e Linux si utilizzano i servizi garantiti dal software di back-up e dalla copia remota dei dati verso la sede C: i dati verranno restorati, in un momento successivo alla ripartenza, su nuovi server che verranno man mano resi disponibili.



segue

WAN Link

Il primo problema riguarda la disponibilità di un accesso ad Internet, dal quale gli utenti potranno ripartire a lavorare sul server e sui dati messi a disposizione dalla restore.

La sede dell'ente, come più volte evidenziato, è collegata ad Internet attraverso una connessione in fibra, con router in comodato di Acantho.

In caso di disastro bisognerà richiedere l'attivazione, normalmente garantita entro 7 giorni dalla richiesta, di una connessione ADSL o HDSL con router a noleggio presso una delle sedi dell'ente verso la sede B di disaster. Una volta ottenuta, il fornitore di assistenza sistemistica provvederà alla riconfigurazione dei server e delle postazioni di lavoro per la ripartenza dei servizi.

Firewall

Nel caso del Comune di Castenaso la riconfigurazione del server comporta anche la riconfigurazione e, di conseguenza, la ripartenza dei servizi di firewall le cui operazioni saranno a carico del CED dell'ente.

Procedure da seguire per affrontare una situazione di disaster recovery

La procedura da seguire, che cercheremo di definire passo a passo, è strettamente legata alle soluzioni tecniche adottate.

Server

Procedure da eseguire per i server di cui è presente il servizio di disaster recovery sul software di back-up dei dati

Si cerca di riassumere in modo sintetico e semplice le attività da eseguire

Tavola 31.: riepilogo procedure di disaster recovery per la sede del Municipio di Castenaso legate ai dati

Per la sede del Municipio: attività a preventivo

1. eseguire giornalmente il back-up dei dati (responsabile è Francesco Capasso)
2. controllare la corretta esecuzione dei back-up (responsabile è Francesco Capasso)
3. controllare due volte alla settimana la buona riuscita dei back-up “disaster copy” presso la sede di disaster (responsabile è Francesco Capasso)
4. controllare che le versioni del software di back-up siano quelle presenti nei CD-ROM di installazione (responsabile è Francesco Capasso)
5. provvedere a centralizzare in luogo definito e sicuro, esterno all’ente, o interno ma in cassaforte ignifuga, CD ROM dei sistemi operativi e dei software di sistema e di back-up, in modo da averli sempre a disposizione in caso di bisogno (responsabile è Francesco Capasso)



segue

Attività da espletare in caso di disastro

1. ordinare al fornitore la necessità di attivare i server “disaster” sui quali far ripartire il servizio, server che, come da accordi devono essere resi disponibili nella sede di disaster entro 3 giorni
2. avvertire del disastro il partner Cedaf perché si tenga pronto ad intervenire (responsabile è Francesco Capasso)
3. definire gli utenti che dovranno ripartire nella sede di disaster (responsabile è Francesco Capasso)
4. provvedere alla reinstallazione dei server Windows 200X e Linux (responsabile è Francesco Capasso)
5. restaurare i dati sul server Windows 200X e Linux (responsabile è Francesco Capasso)
6. installare le postazioni client per detti utenti o permettergli di lavorare da postazioni esistenti (responsabile è Francesco Capasso)
7. ridefinire le stampanti (responsabile è Francesco Capasso)
8. riattivare il sistema di back-up sul nuovo server (responsabile è Francesco Capasso)

Router e Wan Link

Essendo la sede di disaster non collegata ad Internet, in caso di disastro sarà necessario provvedere ad espletare tutte quelle attività che sono necessarie per collegare ad Internet la sede di disaster. Le attività da fare sono le seguenti:

Tavola 32.: riepilogo procedure di disaster recovery per la sede di Castenaso legate ai Wan Link

Attività da espletare in caso di disastro

1. avvertire del disastro il partner LGM perché si tenga ad intervenire (responsabile è Francesco Capasso)
2. avvertire del disastro il partner Cedaf perché si tenga ad intervenire (responsabile è Francesco Capasso)
3. ordinare una nuova connessione ADSL/HDSL Internet verso la sede di disaster a Telecomitalia (responsabile è Francesco Capasso)
4. avvisare il fornitore dei servizi di assistenza sistemistica (Acantho) perché provveda alla riconfigurazione dei servizi HDSL di connessione (responsabile è Francesco Capasso)
5. provvedere alla riconfigurazione dei servizi firewall (responsabile è Francesco Capasso)
6. avvisare il fornitore dei servizi di disaster perché provveda alla riconfigurazione dei server (responsabile è Francesco Capasso)
7. avvisare il fornitore del servizio di disaster della necessità di riconfigurare i servizi di back-up sulla nuova sede temporaneamente attivata (responsabile è Francesco Capasso)
8. Riconfigurare i posti di lavoro per quanto concerne le attività Internet (responsabile è Francesco Capasso)

Documenti aggiuntivi: disciplinare Internet

Nel corso di questi anni il Garante per la protezione dei dati personali, ha emesso una serie di provvedimenti volti a rendere obbligatori alcuni adempimenti ulteriori rispetto al DPS. In particolare con delibera n. 13 del 1 marzo 2007, denominata **“le linee guida del Garante per posta elettronica e internet”** ha disposto che ogni organizzazione si doti di un “Disciplinare interno” che regoli la materia, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori, ecc.) e da sottoporre ad aggiornamento periodico.

Tale disciplinare è stato redatto entro la data di scadenza annuale del DPS, ovvero entro il 31 marzo 2008. Il DPS recepisce quanto disposto da detto disciplinare in materia di gestione di Internet verso la rete interna e gli utenti. Ogni anno viene regolarmente aggiornato entro il 31 marzo.

Amministratori di sistema

Il Garante per la protezione dei dati personali, ha emesso il provvedimento “**Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema**” - 27 novembre 2008, nel quale ha chiesto la nomina ufficiale di coloro che svolgono tale funzione, e l’implementazione di accorgimenti tecnici volti a registrare alcuni eventi della attività degli amministratori di sistema stessi.

Il Comune di Castenaso ha provveduto a nominare ufficialmente le persone interne del settore “Sistemi Informativi”, mentre per tutti coloro che svolgono tale attività presso ditte esterne, si è provveduto alla nomina di tali ditte come responsabili esterni al trattamento, ai sensi dell’art. 29 dlgs 196/2003, con obbligo per tali ditte di tenere traccia su proprio registro del “chi ha fatto cosa”.

Per ciò che concerne invece la registrazione dei log, fatto salvo l’applicazione del principio

1utente amministratore =1 user = 1 password

principio valido anche per le ditte esterne a livello aziendale (ovvero hanno un unico username e provvedono al loro interno alla registrazione di chi ha fatto tale attività), è installato un sistema di logging che trasferisce tali dati presso la società 3CiME Technology Srl, la quale mantiene inalterati tali dati per 1 anno solare dalla loro registrazione. Per l’attività di controllo, 3CiME Technology attiva, su richiesta del titolare o di persona da esso incaricata, un account per la consultazione web dei dati di logging.



Relazione allegata al bilancio

Come da indicazione del Garante per la protezione dei dati personali, nella relazione accompagnatoria al bilancio consuntivo, è citata la redazione e l'aggiornamento del presente Documento Programmatico sulla Sicurezza.



Conclusioni

Il presente documento redatto da AltaVia Consulting non esime il Cliente dalle sue responsabilità. Durante l'analisi si è preso atto delle informazioni che gli incaricati hanno fornito e si sono ordinate nel presente documento.

Sarà anche onere dell'ente tenere aggiornato il presente documento, almeno annualmente, sia affidando ancora l'incarico ad AltaVia Consulting che procedendo autonomamente.

Termini e definizioni

La terminologia relativa alla disciplina della gestione dei rischi di protezione può a volte essere di difficile comprensione. In alcuni casi, un termine noto può essere interpretato in modo diverso da persone diverse. Per questi motivi è importante comprendere le definizioni attribuite dagli autori di questa guida ai termini più importanti in essa contenuti. Molte delle definizioni elencate di seguito sono state originariamente utilizzate all'interno di documenti pubblicati da altre due organizzazioni: la International Standards Organization (ISO) e la Internet Engineering Task Force (IETF). Gli indirizzi dei siti Web di queste organizzazioni sono contenuti nella sezione "Ulteriori informazioni" più avanti in questo capitolo. Nell'elenco riportato di seguito sono illustrati i componenti principali della gestione dei rischi di protezione.

•	Previsione di perdita annua — L'importo totale in denaro che l'organizzazione perderà in un anno se non viene presa alcuna iniziativa per ridurre un rischio.
•	Tasso di occorrenza annuo — Il numero di volte che un rischio si potrebbe verificare nel corso di un anno.
•	Bene — Tutto ciò che ha valore per un'organizzazione, come i componenti hardware e software, i dati, le persone e la documentazione.
•	Disponibilità — La caratteristica di un sistema o di una risorsa di sistema che ne garantisce l'utilizzabilità da parte di un utente autorizzato che ne abbia fatto richiesta. La disponibilità è una delle caratteristiche fondamentali di un sistema sicuro.
•	CIA — Acronimo di Confidentiality, Integrity, Availability (<i>Riservatezza, Integrità e Disponibilità</i>).
•	Riservatezza — La caratteristica in base alla quale un'informazione non viene resa disponibile o divulgata a individui, entità o processi non autorizzati (ISO 7498-2).
•	Controllo — Una modalità organizzativa, procedurale o tecnologica di gestione di un rischio; sinonimo di <i>misura di protezione o contromisura</i> .
•	Analisi costi-benefici — Stima e confronto del valore relativo e del costo associati ai diversi controlli proposti al fine di implementare il controllo più efficace.
•	Supporto alle decisioni — Definizione delle priorità dei rischi sulla base di un'analisi costi-benefici. Il costo sostenuto per la riduzione di un rischio mediante una soluzione di protezione viene confrontato con i benefici che la riduzione del rischio apporta all'azienda.
•	Difesa a più livelli — L'approccio che prevede l'applicazione di più livelli di protezione nel caso in cui il livello di difesa di un singolo componente di protezione non sia sufficiente.

•	Attacco — Sfruttamento di una vulnerabilità al fine di danneggiare le attività o intaccare la protezione delle informazioni aziendali.
•	Esposizione — La divulgazione dannosa e diretta di dati sensibili a un'entità non autorizzata (RFC 2828). Ai fini del processo di gestione dei rischi di protezione, con questa definizione si intende in particolare l'entità del danno a un bene aziendale.
•	Impatto — La perdita di profitti complessiva prevista come conseguenza di un attacco ai danni di un bene.
•	Integrità — La caratteristica dei dati che non hanno subito alterazioni o distruzioni in modo non autorizzato (ISO 7498-2).
•	Riduzione dei rischi — Gestione dei rischi mediante specifiche azioni progettate per affrontare i pericoli ad essi associati.
•	Soluzione di riduzione dei rischi — L'implementazione di un controllo organizzativo, procedurale o tecnologico al fine di gestire un rischio di protezione.
•	Probabilità — La possibilità che un evento si verifichi.
•	Gestione dei rischi qualitativa — Un approccio alla gestione dei rischi che prevede l'assegnazione di un valore relativo ai diversi beni, rischi, controlli e tipi di impatto.
•	Gestione dei rischi quantitativa — Un approccio alla gestione dei rischi che prevede l'assegnazione di un valore numerico oggettivo (ad esempio un valore economico) ai diversi beni, rischi, controlli e tipi di impatto.
•	Reputazione — L'opinione della gente nei riguardi di un'organizzazione; la reputazione di molte aziende ha un valore reale, anche se, essendo un concetto intangibile, è difficilmente quantificabile.
•	Ritorno sull'investimento nella protezione (ROSI) — L'importo totale in denaro che un'organizzazione prevede di risparmiare in un anno grazie all'implementazione di un controllo di protezione.
•	Rischio — La combinazione della probabilità che un evento si verifichi e delle conseguenze associate al verificarsi dell'evento (Guida ISO 73).
•	Valutazione dei rischi — Il processo di identificazione dei rischi e di determinazione dell'impatto ad essi associato.
•	Gestione dei rischi — Il processo che prevede la determinazione di un livello accettabile di rischio, la



segue

	valutazione del livello attuale di rischio, l'adozione di azioni volte a ridurre il rischio a un livello accettabile e il mantenimento di questo livello di rischio.
•	Previsione di perdita singola (SLE) — L'importo totale dei ricavi perduti in seguito a una singola occorrenza del rischio.
•	Pericolo — Una causa potenziale di impatto indesiderato ai danni di un sistema o un'organizzazione (ISO 13335-1).
•	Vulnerabilità — Qualsiasi punto debole, processo amministrativo, azione o esposizione fisica che rende un bene informatico suscettibile di attacco



DISCIPLINARE

sull'utilizzo di Internet, e-mail

ed altri strumenti elettronici

Revisione n° 4 del 15 marzo 2010

1	PREMESSA.....	7
1.1	Finalità	7
1.2	Quadro normativo	7
1.3	Ambito di applicazione	7
1.4	Accordo sindacale.....	7
1.5	Integrazione all’informativa resa al lavoratore	8
1.6	Modalità di pubblicizzazione	8
1.7	Aggiornamento periodico.....	8
2	SCELTE DI FONDO	9
2.1	Garanzie di funzionalità e rispetto della riservatezza	9
2.2	Uso tollerato per fini personali degli strumenti elettronici- Criteri fondamentali.....	9
2.3	Principio di prevenzione	10
2.3.1	Soluzioni organizzative/formative.....	10
2.3.1.1	Ubicazione delle postazioni di lavoro	10
2.3.1.2	Training lavoratori	10
2.3.1.3	Amministratore di sistema e altre figure tecniche	11
3	ATTIVITÀ DI CONTROLLO VIETATA E LECITA.....	12
3.1	Attività di controllo vietata.....	12
3.2	Principi fondamentali dell’attività di controllo lecita	12
3.2.1	Principio di necessità, di pertinenza e di non eccedenza	12
3.2.2	Principio di finalità e di correttezza	12
3.2.3	Valutazione impatto sull’ambiente lavorativo (VIAL).....	13
3.2.4	Attività svolte per finalità di assistenza tecnica ai lavoratori	13
4	MODALITÀ DI UTILIZZO DEI SERVIZI INTERNET	14
4.1	Politica di distribuzione degli accessi Internet	14

4.1.1	Navigazione web e programmi Internet.....	14
4.1.1.1	Accesso ad Internet fornito a tutti i lavoratori.....	14
4.1.1.2	Utilizzo dei programmi che fanno uso di Internet.....	14
4.1.1.3	Regole per il lavoratore per la navigazione in internet	14
4.1.1.4	Attività dell'amministratore di sistema	15
4.1.2	Posta elettronica – Account e-mail	16
4.1.2.1	Utilizzo della Posta Elettronica comunale fornita a tutti i lavoratori	16
4.1.2.2	Utilizzo di account di posta elettronica / alias non nominativi	16
4.1.2.3	Utilizzo dei programmi client di posta elettronica	16
4.1.2.4	Regole per il lavoratore per l'utilizzo della posta elettronica	16
4.1.2.5	Designazione fiduciario del lavoratore e individuazione dei casi di indispensabile accesso da parte dell'amministratore di sistema, con relativa comunicazione al lavoratore.	17
4.1.2.6	Attività dell'amministratore di sistema	17
4.2	Strumento di web / e-mail content filter	18
4.2.1	Navigazione web e programmi Internet.....	19
4.2.1.1	Azioni di filtraggio dei siti web.....	19
4.2.1.2	Blocco dei servizi/applicativi Internet indesiderati	19
4.2.1.3	Blocco del download di file per tipologia	19
4.2.2	Posta Elettronica – Account e-mail.....	19
4.2.2.1	Azioni di filtraggio delle e-mail	19
4.2.2.1.1	Filtro antivirus.....	19
4.2.2.1.2	Filtro antispyware.....	19
4.2.2.1.3	Filtro degli allegati:	19
4.3	Politica di tolleranza dell'uso personale di Internet.....	20
4.3.1	Navigazione web dalle postazioni di lavoro	20
4.3.2	Utilizzo dell'account di posta elettronica comunale nominativo PROF per uso personale dalle postazioni di lavoro.....	20

4.3.3	Utilizzo di internet e della posta elettronica da parte dell'Amministratore di Sistema.....	20
4.4	Dati conservati dal sistema relativamente all'utilizzo degli strumenti elettronici.....	20
4.4.1	Internet.....	20
4.4.1.1	Navigazione internet	20
4.4.1.2	Cronologia delle pagine web visitate.....	21
4.4.1.3	Memoria cache delle pagine web visitate	21
4.4.1.4	Cookies	21
4.4.1.5	Policy particolari	21
4.4.2	E-mail	22
4.4.2.1	Backup file di posta.....	22
5	ULTERIORI NORME COMPORTAMENTALI	23
5.1	Custodia dotazione hardware	23
5.2	Sicurezza in materia di autenticazione dei lavoratori	24
5.3	Modalità di memorizzazione di documenti sui sistemi comunali	24
5.4	Installazione software	25
5.5	Attività dell'amministratore di sistema	26
6	MODALITÀ DEI CONTROLLI.....	28
6.1	Internet.....	28
6.2	E-mail.....	29
6.3	File system	29
7	PROCEDURE IN CASO DI CESSAZIONE DEL RAPPORTO LAVORATIVO	30
7.1	Documenti memorizzati sui sistemi comunali.....	30
7.2	E-mail.....	30
7.3	Tracce elettroniche ("log")	30
8	SANZIONI APPLICABILI E RELATIVE PROCEDURE.....	31
9	ALLEGATO A - ELENCO DEGLI STRUMENTI SOFTWARE UTILIZZATI PER L'ATTIVITÀ DI ASSISTENZA TECNICA INFORMATICA	33

10	ALLEGATO B - ELENCO DEI PROGRAMMI A DISPOSIZIONE PER LA NAVIGAZIONE IN INTERNET E PER LA POSTA ELETTRONICA	34
10.1	NAVIGAZIONE IN INTERNET.....	34
10.2	POSTA ELETTRONICA	34
11	ALLEGATO C - CATEGORIE DI FILTRAGGIO DEI SITI WEB	35
12	ALLEGATO D - ELENCO DELLE TIPOLOGIE DI FILE BLOCCATI IN DOWNLOAD DA INTERNET	36
12.1	ESTENSIONI DI FILE	36
12.2	TIPOLOGIE MIME	37
13	ALLEGATO E - ELENCO DELLE ESTENSIONI DI FILE BLOCCATI COME ALLEGATI ALLE E-MAIL.....	38
14	ALLEGATO F - ISTRUZIONI OPERATIVE PER LA CANCELLAZIONE DELLA CRONOLOGIA DELLE PAGINE WEB VISITATE	39
15	ALLEGATO G - ISTRUZIONI OPERATIVE PER LA CANCELLAZIONE DELLA MEMORIA CACHE DELLE PAGINE WEB VISITATE	40
16	ALLEGATO H - ISTRUZIONI OPERATIVE PER LA CANCELLAZIONE DEI COOKIES.....	41
17	ALLEGATO I - ISTRUZIONI OPERATIVE SU COME BLOCCARE IL COMPUTER.....	42
17.1	Blocco del computer.....	42
17.2	Sblocco del computer	43
18	ALLEGATO J - ISTRUZIONI OPERATIVE SULL'UTILIZZO DEL SOFTWARE ANTIVIRUS	44
19	ALLEGATO K - ISTRUZIONI OPERATIVE SULL'UTILIZZO DEL MESSAGGIO DI ASSENZA DALL'UFFICIO	47
19.1	Lotus iNotes.....	47
19.2	Lotus Notes.....	50
20	ALLEGATO L – ISTRUZIONI OPERATIVE SULLA CANCELLAZIONE DI UNA E-MAIL INDESIDERATA DAL DATABASE DI POSTA	53
20.1	Lotus iNotes.....	53
20.2	Lotus Notes.....	55
21	ALLEGATO M - UNITÀ DI RETE	57
21.1	Unità di rete per il salvataggio di file e dati - esclusi i dati sensibili o giudiziari.....	57
21.2	Altre unità di rete - da non utilizzare per salvare dati.....	57

22 ALLEGATO N – AVVERTIMENTO AUTOMATICO PER LE E-MAIL..... 59

1 PREMESSA

1.1 Finalità

Il disciplinare chiarisce le policy predisposte e applicate dal Comune di Castenaso relativamente all'utilizzo di alcuni strumenti elettronici nel contesto lavorativo; esplicita altresì i dati personali che sono o possono essere tracciati sui sistemi per effetto dell'utilizzo di alcuni strumenti elettronici; indica i possibili controlli leciti esercitabili dal Comune di Castenaso circa l'effettivo utilizzo degli strumenti e il rispetto delle policy nonché, per i casi di eventuale violazione, le procedure e le sanzioni applicabili.

1.2 Quadro normativo

Costituiscono riferimenti normativi fondamentali del disciplinare:

- la legge n. 300/1970 (Statuto dei lavoratori), in particolare gli artt. 4 e 8;
- il decreto legislativo n. 196/2003 (Codice in materia di protezione dei dati personali);
- il provvedimento del Garante per la protezione dei dati personali n. 13/2007.

Nella redazione del disciplinare si è inoltre considerata la giurisprudenza formatasi sulle predette disposizioni legislative, così come sono state tenute presenti le ulteriori pronunce dell'Autorità Garante.

1.3 Ambito di applicazione

Il presente disciplinare riguarda l'utilizzo di:

- internet
- e-mail
- file system
- software per la manutenzione in remoto
- sicurezza in materia di autenticazione degli utenti
- salvataggio dei dati, unità di rete ed utilizzo di supporti removibili
- allegati tecnici (blocco del pc, uso del sw antivirus, ecc.)

1.4 Accordo sindacale

Nel rispetto del quadro normativo di riferimento sopra richiamato, ed in particolare dell'art. 4 della legge n. 300/1970 nonché del Provvedimento del Garante n. 13/2007, il disciplinare è stato sottoposto all'attenzione delle rappresentanze sindacali, che, in data 25/09/2008 lo hanno approvato come risulta riportato nel verbale della seduta della Delegazione Trattante conservato in atti.

è stato sottoposto all'attenzione delle rappresentanze sindacali, le quali in data __/__/____ hanno sottoscritto il necessario accordo (inserire eventuali riferimenti), pubblicato nelle consuete forme;

- non avendo ottenuto l'accordo delle rappresentanze sindacali, è stato autorizzato dalla DLP- Direzione Provinciale del Lavoro di _____ - Ispettorato del Lavoro, con provvedimento autorizzativo prot. n. _____ del ____/____/____;

L'accordo sindacale/l'autorizzazione della DLP permettono pertanto al Comune di Castenaso di effettuare i controlli leciti descritti in prosieguo.

1.5 Integrazione all'informativa resa al lavoratore

Circa l'eventuale trattamento di dati personali del lavoratore effettuato per verificare il corretto utilizzo di alcuni strumenti elettronici, il disciplinare costituisce un'integrazione alla più generale informativa sul trattamento dei dati personali resa ai sensi dell'art. 13 del decreto legislativo n. 196/2003, la quale è sempre disponibile sul disco di rete F:\CASTENASO\ visibile da tutti i dipendenti comunali in possesso di un profilo di rete e nella bacheca del Settore Risorse Umane del Comune di Castenaso.

1.6 Modalità di pubblicizzazione

In considerazione dell'importanza che riveste e della delicatezza di alcuni aspetti considerati, il disciplinare è pubblicato adeguatamente, anche nel rispetto dello Statuto dei lavoratori (cfr. art. 7 *"Le norme disciplinari relative alle sanzioni alle infrazioni in relazione alle quali ciascuna di esse può essere applicata ed alle procedure di contestazione delle stesse, devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti"*).

Il Comune di Castenaso dispone a tal fine che il disciplinare sia:

- affisso nella bacheca del Settore Risorse Umane del Comune di Castenaso;
- reso disponibile sul disco di rete F:\CASTENASO\ visibile da tutti i dipendenti comunali in possesso di un profilo di rete;
- comunicato a mezzo e-mail a tutti i lavoratori raggiunti da tale servizio, mediante invio del link per accedere alla Bacheca elettronica suddetta.

1.7 Aggiornamento periodico

Il disciplinare viene aggiornato periodicamente, con frequenza almeno annuale, in considerazione di:

- introduzione di nuovi strumenti elettronici, rilevanti per le finalità del disciplinare;
- modifiche e/o innovazioni di carattere normativo o giurisprudenziale;
- modifiche e/o innovazioni di carattere tecnico-informatico;
- esperienze maturate, nel periodo di riferimento, in applicazione del disciplinare;
- nuove esigenze di sicurezza, produzione, organizzazione che giustifichino una revisione del disciplinare;
- diversa distribuzione delle risorse informatiche e telematiche;
- aggiornamento piani di formazione.

2 SCELTE DI FONDO

2.1 Garanzie di funzionalità e rispetto della riservatezza

Il Comune di Castenaso deve assicurare la funzionalità e il corretto impiego degli strumenti elettronici da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, sia pure nel rispetto della disciplina in tema di diritti e relazioni sindacali. A tal fine, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità, il Comune di Castenaso adotta idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati (il quadro di tali misure di sicurezza sempre disponibile sul disco di rete F:\CASTENASO\ visibile da tutti i dipendenti comunali in possesso di un profilo di rete).

In tale contesto, il Comune di Castenaso considera che l'utilizzo di Internet, dell' e-mail e di altri strumenti elettronici da parte dei lavoratori può generare, e di norma genera, informazioni – talora addirittura “sensibili”- che possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi.

Il Comune è ben consapevole, poi, che il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati.

Il presente disciplinare intende perciò precisare modi e forme con le quali, in una cornice di reciproci diritti e doveri, possa essere meglio assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali, da un lato, e il giusto perseguimento dei fini propri del Comune, dall'altro.

2.2 Uso tollerato per fini personali degli strumenti elettronici- Criteri fondamentali

Nel contesto lavorativo del Comune di Castenaso è tollerato un moderato e sporadico utilizzo degli strumenti elettronici per fini personali da parte dei lavoratori, finalizzato a:

- navigazione su Internet
- utilizzo dell' account e-mail comunale
- archiviazione sui sistemi comunali di documenti personali
- chiamate telefoniche.

Tale uso personale tollerato:

- deve rispettare le ulteriori regole e limiti stabilite dal presente disciplinare;
- deve essere moderato;
- deve essere, almeno di regola, attuato nelle ordinarie pause dell'attività lavorativa o fuori dall'orario di lavoro (variabile tale orario a seconda del servizio programmato), ma sempre e comunque in giornate lavorative: in sostanza non è possibile recarsi al lavoro in giorno non lavorativo per eseguire tali attività, e ci si può soffermare fuori orario nei limi di una mezz'ora antecedente o successiva l'orario di servizio;

- non deve comunque entrare in conflitto, ostacolare o impedire il corretto svolgimento delle prestazioni lavorative;
- deve essere lecito, ossia non confliggere con alcuna norma imperativa dell'ordinamento;
- può essere sempre inibito in ragione di esigenze di sicurezza, di produzione, di organizzazione o altre esigenze comunali.

2.3 Principio di prevenzione

Il Comune di Castenaso riconosce che il primo e miglior modo per contemperare gli interessi del Comune e del lavoratore, per i fini qui in esame, è l'adozione di misure tese a prevenire comportamenti scorretti o illeciti, più che intervenire dopo che detti comportamenti si siano verificati.

Tale principio suggerisce:

- sotto il profilo tecnico-informatico, di adottare misure *tecnologiche* volte a prevenire comportamenti scorretti e contestualmente a minimizzare l'uso di dati identificativi (c.d. *privacy enhancing technologies–PETs*). Le misure sono differenziate a seconda della tecnologia impiegata e sono perciò indicate in prosieguo in modo distinto per ciascuno strumento utilizzato;
- sotto il profilo organizzativo, di adottare tutte le soluzioni idonee a sconsigliare e rendere meno agevoli i comportamenti scorretti che si vogliono prevenire. Le misure organizzative adottate da Comune di Castenaso sono indicate nel presente paragrafo.

2.3.1 Soluzioni organizzative/formative

2.3.1.1 Ubicazione delle postazioni di lavoro

Il Comune di Castenaso valuta l'opportunità di collocare e configurare , ove possibile, le postazioni di lavoro in modo da disincentivare utilizzi scorretti degli strumenti elettronici. Rappresentano esempi pratici di tale valutazione:

- la collocazione delle postazioni di lavoro in aree non isolate;
- le scelte dell'orientamento dei monitor, comunque nel rispetto delle altre normative vigenti (decreto legislativo n. 626/1994 e ss.mm.; decreto legislativo n. 196/2003)
- le disposizioni relative all'apertura delle porte dei locali in cui sono collocati gli strumenti elettronici;
- le disposizioni relative alla condivisione, da parte di due o più lavoratori, dei medesimi strumenti elettronici.

2.3.1.2 Training lavoratori

E' interesse del Comune di Castenaso, oltre che del lavoratore, garantire una puntuale formazione circa diritti, obblighi, responsabilità inerenti politiche e controlli sull'utilizzo degli strumenti elettronici nel rapporto di lavoro.

Il Comune di Castenaso predispone ed aggiorna periodicamente perciò, nell'ambito del Piano di Formazione del Personale adottato annualmente dalla Giunta, un piano di formazione in aula e/o in e-learning avente ad oggetto i seguenti contenuti:

- il Decreto Legislativo 196/2003 e la figura del Garante
- i profili sulla disciplina di protezione dei dati
- le responsabilità degli incaricati al trattamento dei dati
- I rischi che incombono sui dati e relative misure di prevenzione, contrasto e mitigazione dei danni
- la tutela della privacy nel rapporto di lavoro
- le regole in vigore, dallo Statuto dei lavoratori al Provvedimento del Garante n. 13/2007
- il disciplinare interno del Comune di Castenaso

La pianificazione annuale degli interventi formativi è contenuta nel Piano di Formazione del Personale deliberato annualmente dalla Giunta Comunale

2.3.1.3 Amministratore di sistema e altre figure tecniche

Il ruolo di amministratore di sistema è oggettivamente strategico per l'efficienza dei sistemi informativi comunali e al contempo delicato, anche per i fini considerati dal presente disciplinare.

A garanzia del lavoratore, pertanto, il Comune di Castenaso ritiene necessario:

- definire precise regole di condotta dei soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi;
- garantire a tali figure un'attività formativa ad hoc sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

Nel caso di eventuali interventi per esigenze di manutenzione del sistema, il Comune di Castenaso adotta ogni misura volta a prevenire l'indebito accesso a dati personali presenti in cartelle o spazi di memoria assegnati a lavoratori.

La pianificazione annuale degli interventi formativi è contenuta nel Piano di Formazione del Personale deliberato annualmente dalla Giunta Comunale.

3 ATTIVITÀ DI CONTROLLO VIETATA E LECITA

3.1 Attività di controllo vietata

Il Comune di Castenaso rispetta le leggi vigenti e i provvedimenti che vietano il trattamento effettuato mediante sistemi *hardware* e *software* preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire sistematicamente l'attività dei lavoratori. Nel contesto lavorativo del Comune di Castenaso non si effettuano ad esempio:

- lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
- riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
- lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- analisi occulta di computer affidati in uso.

3.2 Principi fondamentali dell'attività di controllo lecita

L'attività di eventuale controllo, lecitamente svolta dal Comune di Castenaso ai sensi del presente disciplinare, si attiene in ogni caso ai seguenti fondamentali principi:

3.2.1 Principio di necessità, di pertinenza e di non eccedenza

I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite, osservando altresì il principio di pertinenza e non eccedenza. Il Comune raccoglie e tratta i dati nella misura meno invasiva possibile; le eventuali attività di controllo sono svolte solo da soggetti preposti e sono mirate sull'area individuata come "di rischio".

3.2.2 Principio di finalità e di correttezza

I trattamenti sono effettuati per finalità determinate, esplicite e legittime. Le finalità perseguite dal Comune di Castenaso riguardano o possono riguardare, caso per caso:

- sicurezza sul lavoro
- sicurezza dei sistemi e relativa risoluzione di problemi tecnici
- esigenze di organizzazione
- esigenze di produzione
- rispetto di obblighi legali
- tutela del Comune

In nessun caso il Comune di Castenaso persegue finalità di controllo a distanza diretto, sistematico e/o intenzionale dell'attività dei lavoratori.

Le caratteristiche essenziali dei trattamenti sono rese note ai lavoratori (art. 11, comma 1, lett. a), del decreto legislativo n. 196/2003), anche considerando che le tecnologie dell'informazione (in

modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere –spesso all’insaputa o senza la piena consapevolezza del lavoratore- trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa.

3.2.3 Valutazione impatto sull’ambiente lavorativo (VIAL)

Al fine di ponderare adeguatamente, prima dell’eventuale installazione, l'impatto sui diritti dei lavoratori di nuovi strumenti suscettibili di consentire il controllo a distanza, e del trattamento di dati personali che ne possa derivare, il Comune di Castenaso procede –caso per caso- ad una specifica valutazione dell’impatto sull’ambiente lavorativo, da svolgersi alla luce delle norme vigenti, della giurisprudenza formatasi nonché dei principi del presente disciplinare.

La valutazione è predisposta dal Responsabile del Trattamento di propria iniziativa o su richiesta di altro Responsabile del trattamento ovvero su richiesta del Segretario Comunale. La valutazione è contenuta in un Documento di Valutazione dell’Impatto sull’Ambiente Lavorativo (DocVIAL) che contiene almeno:

- le caratteristiche del nuovo strumento che si intende installare
- le ragioni che impongono o suggeriscono l’installazione, e le finalità perseguite
- i tipi di dati che saranno raccolti a seguito dell’installazione del nuovo strumento
- le misure suggerite per garantire il miglior equilibrio con i diritti dei lavoratori.

Il DocVIAL è conservato a cura del Responsabile del Trattamento, e costituisce riferimento per l’aggiornamento periodico del presente disciplinare.

3.2.4 Attività svolte per finalità di assistenza tecnica ai lavoratori

Ai soli fini di prestare assistenza tecnica informatica ai lavoratori, il Comune utilizza alcuni software che permettono all’amministratore di sistema di vedere in tempo reale le attività svolte dal lavoratore all’interno della propria sessione di lavoro ed eventualmente di intervenire attivamente. L’attivazione di tale funzionalità può essere richiesta solamente da parte degli amministratori di sistema e solo quando strettamente necessario per poter svolgere l’attività di assistenza tecnica informatica e DEVE ESSERE sottoposta ad un preventivo e contestuale consenso da parte del lavoratore

Gli strumenti software utilizzati dagli amministratori di sistema per svolgere l’attività di assistenza tecnica informatica sono elencati nell’ALLEGATO A - ELENCO DEGLI STRUMENTI SOFTWARE UTILIZZATI PER L’ATTIVITÀ DI ASSISTENZA TECNICA INFORMATICA al presente disciplinare.

4 MODALITÀ DI UTILIZZO DEI SERVIZI INTERNET

4.1 Politica di distribuzione degli accessi Internet

4.1.1 Navigazione web e programmi Internet

4.1.1.1 Accesso ad Internet fornito a tutti i lavoratori

Il Comune di Castenaso ha deciso di fornire l'accesso ad Internet a tutti i lavoratori e collaboratori che per il corretto adempimento delle proprie mansioni abbiano necessità di utilizzare strumenti elettronici, indipendentemente dal settore di impiego del lavoratore stesso.

4.1.1.2 Utilizzo dei programmi che fanno uso di Internet

Il Comune di Castenaso mette a disposizione dei lavoratori i programmi necessari per navigare in internet ed utilizzare i servizi internet necessari per l'attività lavorativa. Tali programmi sono stati testati e validati dai Sistemi Informativi del Comune. Onde evitare problemi di malfunzionamento, sicurezza e instabilità dei sistemi, i lavoratori sono tenuti ad utilizzare solamente il software fornito. L'elenco dei programmi a disposizione dei lavoratori per la navigazione in internet è disponibile nell'ALLEGATO B - ELENCO DEI PROGRAMMI A DISPOSIZIONE PER LA NAVIGAZIONE IN INTERNET E PER LA POSTA ELETTRONICA al presente disciplinare.

4.1.1.3 Regole per il lavoratore per la navigazione in internet

Per la navigazione in internet il lavoratore deve attenersi alle seguenti regole:

- non è consentita la navigazione in siti con contenuti i cui contenuti siano compresi nelle categorie di filtraggio di cui all'ALLEGATO C - CATEGORIE DI FILTRAGGIO DEI SITI WE al presente disciplinare;
- non è consentita la navigazione in siti di posta elettronica web se non attinenti allo svolgimento dell'attività lavorativa;
- non è consentito l'utilizzo di servizi web proxy o di servizi web di anonimizzazione al fine di eludere i filtri e le regole di sicurezza implementate dal Comune;
- non è consentita l'effettuazione di transazioni finanziarie ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi autorizzati o previsti dai regolamenti comunali e con il rispetto delle normali procedure di acquisto o nell'ambito del mercato elettronico della Pubblica Amministrazione;
- non è consentito il download, la copia, il salvataggio, l'installazione o l'utilizzo di software prelevato da siti internet, se non espressamente autorizzato dall'amministratore di sistema;
- non è consentito l'uso di software di condivisione di risorse (peer to peer o shared);
- non è consentito l'uso di software di telefonia su ip (VOIP), di instant messaging o di videoconferenza se non espressamente autorizzati dall'amministratore di sistema;
- è vietata ogni forma di registrazione a nome del Comune o fornendo i dati relativi a e-mail Comunale a siti i cui contenuti non siano legati all'attività lavorativa;

- non è permessa la partecipazione per motivi non professionali a forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book nemmeno utilizzando pseudonimi (o nicknames);
- non è consentita il download, la copia o il salvataggio di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- ferme restando le attività dell'amministratore di sistema di implementazione, configurazione e gestione dei software antivirus presenti nel sistema informatico, spetta al lavoratore sottoporre a verifica tutti i file di provenienza incerta o esterna scaricati da internet, ancorché attinenti all'attività lavorativa, tramite gli strumenti antivirus in dotazione. Le istruzioni operative sull'utilizzo del software antivirus sono contenute nell'ALLEGATO J - ISTRUZIONI OPERATIVE SULL'UTILIZZO DEL SOFTWARE ANTIVIRUS al presente disciplinare.

4.1.1.4 Attività dell'amministratore di sistema

L'amministratore di sistema provvede ad inibire la navigazione in siti inutili per la produttività aziendale ed, in particolare, quelli potenzialmente lesivi per l'infrastruttura. A tal fine sono identificate diverse categorie di siti sottoposti a blocco. L'elenco delle categorie di filtraggio dei siti web è contenuto nell'ALLEGATO C - CATEGORIE DI FILTRAGGIO DEI SITI WEB al presente disciplinare. Ferme restando queste regole generali e vista la rapidità di cambiamento dei siti web, di internet ed in generale delle tecnologie informatiche, l'amministratore di sistema provvede periodicamente ad aggiornare le categorie di siti bloccati.

Tramite opportuni filtri è inoltre bloccata la navigazione in siti appartenenti alle categorie sopra indicate sia basandosi su una lista di siti proibiti (black list), sia basandosi sull'analisi del contenuto (ad esempio impedendo la navigazione in pagine che contengono determinate parole o immagini).

Inoltre l'amministratore di sistema provvede ad inibire il download di particolari categorie di file che possano pregiudicare la sicurezza o il funzionamento del sistema informatico operando anche in maniera selettiva (ad esempio per sito o dominio oppure per determinate categorie di utenti). L'elenco delle estensioni e l'elenco delle categorie MIME di file bloccati in download da internet sono contenuti rispettivamente nell'ALLEGATO D - ELENCO DELLE TIPOLOGIE DI FILE BLOCCATI IN DOWNLOAD DA INTERNET al presente disciplinare. Ferme restando queste regole generali e vista la rapidità di cambiamento delle tecnologie informatiche, l'amministratore di sistema provvede periodicamente ad aggiornare le categorie di file bloccati.

L'amministratore di sistema provvede ad implementare, configurare e gestire uno o più software antivirus in grado di proteggere l'infrastruttura informatica da virus e più in generale da malware (un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito). Tali software antivirus, in base alle configurazioni effettuate dall'amministratore di sistema, sono in grado automaticamente di analizzare i file che il lavoratore scarica attraverso la navigazione in internet, di rilevare le infezioni da virus informatici e di riparare, mettere in quarantena o eventualmente eliminare i file infetti.

4.1.2 Posta elettronica – Account e-mail

4.1.2.1 Utilizzo della Posta Elettronica comunale fornita a tutti i lavoratori

Il Comune di Castenaso ha deciso di fornire un account di Posta Elettronica a tutti i lavoratori e collaboratori che per il corretto adempimento delle proprie mansioni abbiano necessità di utilizzare strumenti elettronici, indipendentemente dal settore di impiego del lavoratore stesso. Tutti i lavoratori avranno quindi un **account di posta elettronica comunale nominativo PROFESSIONALE** (di seguito, solo: PROF) di norma nel formato *nome.cognome@comune.castenaso.bo.it*

4.1.2.2 Utilizzo di account di posta elettronica / alias non nominativi

In alcuni casi, in aggiunta all'account di cui al punto precedente, il Comune di Castenaso ha deciso di utilizzare account di posta elettronica comunali NON nominativi, che fanno riferimento agli uffici. Ad esempio:

- urp@comune.castenaso.bo.it
- segreteria@comune. castenaso.bo.it
- finanze@comune. castenaso.bo.it
- biblio@comune. castenaso.bo.it
- edp@comune. castenaso.bo.it
- demogr @comune. castenaso.bo.it
- ecc.

4.1.2.3 Utilizzo dei programmi client di posta elettronica

Il Comune di Castenaso mette a disposizione dei lavoratori i programmi necessari per l'utilizzo della posta elettronica per l'attività lavorativa. Tali programmi sono stati testati e validati dai Sistemi Informativi del Comune. Onde evitare problemi di malfunzionamento, sicurezza e instabilità dei sistemi, i lavoratori sono tenuti ad utilizzare solamente il software fornito. L'elenco dei programmi a disposizione dei lavoratori per l'utilizzo della posta elettronica è disponibile nell'ALLEGATO B - ELENCO DEI PROGRAMMI A DISPOSIZIONE PER LA NAVIGAZIONE IN INTERNET E PER LA POSTA ELETTRONICA al presente disciplinare.

4.1.2.4 Regole per il lavoratore per l'utilizzo della posta elettronica

Per l'utilizzo della posta elettronica, fermo restando l'obbligo di rispetto del segreto postale e delle norme che regolano il rapporto di lavoro dei dipendenti, il lavoratore si deve attenere alle seguenti regole:

- non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- poiché la posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei, l'invio tramite tale mezzo di documenti di lavoro "strettamente riservati" è sconsigliato e comunque va valutato con particolare attenzione;

- non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum o mail-list se non per motivi inerenti l'attività lavorativa svolta;
- non è consentita (se non è stata espressamente indicata nella lettera di incarico) la trasmissione a mezzo di posta elettronica, di dati sensibili e/o giudiziari, il cui trattamento con mezzi elettronici deve avvenire secondo le modalità descritte ai punti successivi e all'allegato tecnico della presente policy;
- non è consentito l'invio di pubblicità di qualunque tipo, via posta elettronica aziendale, sia all'interno che all'esterno dell'ente;
- i dati sensibili e/o giudiziari che pervenissero via posta elettronica possono solo essere conservati nelle risorse predisposte dai sistemi informatici e debbono essere immediatamente cancellati dalle caselle di posta;
- ferme restando le attività dell'amministratore di sistema di implementazione, configurazione e gestione dei software antivirus presenti nel sistema informatico, spetta al lavoratore sottoporre a verifica tutti i file di provenienza incerta o esterna presenti come allegati nella posta in ingresso, ancorché attinenti all'attività lavorativa, tramite gli strumenti antivirus in dotazione. Le istruzioni operative sull'utilizzo del software antivirus sono contenute nell'ALLEGATO J - ISTRUZIONI OPERATIVE SULL'UTILIZZO DEL SOFTWARE ANTIVIRUS al presente disciplinare.

4.1.2.5 Designazione fiduciario del lavoratore e individuazione dei casi di indispensabile accesso da parte dell'amministratore di sistema, con relativa comunicazione al lavoratore.

In previsione della possibilità che in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, ciascun lavoratore, inviando richiesta scritta ai responsabili del trattamento, può delegare un altro lavoratore a verificare, su richiesta del titolare o dei responsabili, il contenuto dei messaggi e a inoltrare al titolare o ai responsabili del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Qualora tale delega non sia stata espressa, le predette operazioni di verifica e inoltramento sono effettuate dall'amministratore di sistema, sempre su richiesta del titolare o dei responsabili. A cura del titolare del trattamento, di tale attività viene redatto apposito verbale e viene informato il lavoratore tramite posta elettronica oppure, qualora non possibile, mediante comunicazione scritta.

4.1.2.6 Attività dell'amministratore di sistema

L'amministratore di sistema mette a disposizione dei lavoratori una funzionalità tramite la quale inviare automaticamente, in caso di assenza programmata, messaggi di risposta per indicare un altro soggetto a cui fare riferimento o altre modalità di contatto dell'Ente. Le istruzioni operative sull'uso del messaggio di assenza dall'ufficio sono contenute nell'ALLEGATO K – ISTRUZIONI OPERATIVE SULL'UTILIZZO DEL MESSAGGIO DI ASSENZA UFFICIO al presente disciplinare

In caso di eventuali assenze non programmate (ad es., per improvvisa malattia), o di emergenze, qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail), il Comune, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale l'amministratore di sistema

l'attivazione di un analogo accorgimento, avvertendo il lavoratore tramite posta elettronica oppure, qualora non possibile, mediante comunicazione scritta.

L'amministratore di sistema mette in opera le necessarie funzionalità affinché tutti i messaggi di posta elettronica contengano un avvertimento automatico ai destinatari, sul modello di quello indicato nell'ALLEGATO N – AVVERTIMENTO AUTOMATICO PER LE E-MAIL, nel quale sia dichiarata la natura professionale dell'account di posta, il possibile utilizzo del medesimo da parte di più soggetti appartenenti al settore/all'area e la conseguente possibile ricezione / consultazione da parte di più soggetti appartenenti al Comune.

Inoltre l'amministratore di sistema provvede ad inibire particolari categorie di allegati ai messaggi di posta elettronica che possano pregiudicare la sicurezza o il funzionamento del sistema informatico operando anche in maniera selettiva (ad esempio per sito o dominio oppure per determinate categorie di utenti). L'elenco delle estensioni di file bloccati come allegati alle e-mail è contenuto nell'ALLEGATO E - ELENCO DELLE ESTENSIONI DI FILE BLOCCATI COME ALLEGATI ALLE E-MAIL al presente disciplinare. Ferme restando queste regole generali e vista la rapidità di cambiamento delle tecnologie informatiche, l'amministratore di sistema provvede periodicamente ad aggiornare le categorie degli allegati bloccati.

L'amministratore di sistema provvede ad implementare, configurare e gestire uno o più software antivirus in grado di proteggere l'infrastruttura informatica da virus e più in generale da malware (un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito). Tali software antivirus, in base alle configurazioni effettuate dall'amministratore di sistema, sono in grado automaticamente di analizzare allegati ai messaggi di posta elettronica, di rilevare le infezioni da virus informatici e di riparare, mettere in quarantena o eventualmente eliminare gli allegati infetti.

Per i soli fini di risoluzione di gravi problematiche o malfunzionamenti tecnici relativi all'utilizzo della posta elettronica e solamente a seguito di un'esplicita e contestuale autorizzazione scritta da parte del lavoratore, l'amministratore di sistema ha la possibilità di accedere alla casella di posta elettronica del lavoratore stesso, secondo le modalità operative e di documentazione sopra riportate.

Inoltre l'amministratore di sistema può definire limitazioni della dimensione della casella di posta alle esigenze di spazio disco aziendali. Raggiunto tale limite, l'utente è costretto ad archiviare o a cancellare posta, pena il non riuscire a ricevere altri messaggi, come avviene nella mailbox pubbliche.

4.2 Strumento di web / e-mail content filter

Il Comune di Castenaso, onde garantire che le descritte policy per l'utilizzo di Internet siano effettivamente rispettate dai lavoratori, si è dotato di strumenti finalizzati a prevenire un utilizzo indebito dei servizi Internet mediante azioni di filtering (filtro), in relazione sia alla navigazione che all'utilizzo dell'e-mail.

4.2.1 Navigazione web e programmi Internet

Con riferimento alla navigazione su Internet, il Comune utilizza software implementati sul firewall che presidia la rete comunale. Tale strumento è configurato per effettuare:

4.2.1.1 Azioni di filtraggio dei siti web

L'elenco delle categorie di filtraggio dei siti web è contenuto nell'ALLEGATO C - CATEGORIE DI FILTRAGGIO DEI SITI WE al presente disciplinare.

4.2.1.2 Blocco dei servizi/applicativi Internet indesiderati

Ad eccezione della navigazione in internet (su porte 80-HTTP e 443-HTTPS) sono bloccati gli accessi a tutti i servizi internet (es: instant messaging, voip, skype, peer to peer, giochi on line, ecc.).

4.2.1.3 Blocco del download di file per tipologia

L'elenco delle tipologie di file bloccati in download da internet è contenuto nell'ALLEGATO D - ELENCO DELLE TIPOLOGIE DI FILE BLOCCATI IN DOWNLOAD DA INTERNET al presente disciplinare.

4.2.2 Posta Elettronica – Account e-mail

Il Comune di Castenaso, onde garantire un elevato livello di sicurezza del sistema informativo si è dotato, al solo scopo di filtraggio, di uno strumento che regolamenti l'utilizzo della posta elettronica.

4.2.2.1 Azioni di filtraggio delle e-mail

4.2.2.1.1 Filtro antivirus

Con riferimento alla posta elettronica, il Comune utilizza filtri antivirus (ovvero finalizzati ad impedire la ricezione di allegati potenzialmente pericolosi).

4.2.2.1.2 Filtro antispam

Con riferimento alla posta elettronica, il Comune utilizza filtri antispam, antiphishing e antipharming (ossia, finalizzati a filtrare la posta elettronica non desiderata).

4.2.2.1.3 Filtro degli allegati:

Con riferimento alla posta elettronica, il Comune utilizza filtri finalizzati a limitare i messaggi con le seguenti caratteristiche:

- **dimensioni:** sono bloccate le e-mail o i singoli allegati che superano la dimensione di 100 MB; viene ritardata ad un orario notturno la consegna delle e-mail che superano la dimensione di 10 MB o inviate ad un numero notevole di destinatari (ad esempio le mailing list).
- **estensione dei files allegati:** sono bloccati gli allegati alle e-mail con estensione presente nell'elenco contenuto nell'ALLEGATO E - ELENCO DELLE ESTENSIONI DI FILE BLOCCATI COME ALLEGATI ALLE E-MAIL al presente disciplinare.

4.3 Politica di tolleranza dell'uso personale di Internet

4.3.1 Navigazione web dalle postazioni di lavoro

Il Comune di Castenaso consente l'utilizzo moderato e sporadico di Internet, inteso come pura navigazione web, per uso personale dalla propria postazione di lavoro con le limitazioni indicate al paragrafo 4.1 fermo restando l'utilizzo da parte del Comune di Castenaso degli strumenti di filtro di cui al paragrafo 4.2.

4.3.2 Utilizzo dell'account di posta elettronica comunale nominativo PROF per uso personale dalle postazioni di lavoro

Il Comune di Castenaso consente l'utilizzo dell'account di posta elettronica comunale nominativo PROF per uso personale dalla propria postazione di lavoro con le limitazioni indicate al paragrafo 4.1 fermo restando l'utilizzo da parte del Comune di Castenaso degli strumenti di filtro di cui al paragrafo 4.2.

4.3.3 Utilizzo di internet e della posta elettronica da parte dell'Amministratore di Sistema

L'amministratore di sistema, pur essendo tenuto di norma al rispetto delle regole indicate al paragrafo 4.1, qualora strettamente necessario per ragioni di controllo, sviluppo di nuove funzionalità, gestione ed amministrazione del sistema è autorizzato a derogare alle limitazioni sull'utilizzo dei servizi internet e della posta elettronica.

In via esemplificativa, tale deroga può riguardare:

- la verifica della natura di taluni siti internet, qualora ciò non possa agevolmente desumersi dai dati di traffico;
- l'utilizzo di siti di posta elettronica web per la verifica del funzionamento dei servizi di posta elettronica interni;
- il download, la copia, il salvataggio, l'installazione e l'utilizzo di software prelevato da siti internet nel rispetto delle normative sul copyright e sul diritto d'autore;

4.4 Dati conservati dal sistema relativamente all'utilizzo degli strumenti elettronici

4.4.1 Internet

4.4.1.1 Navigazione internet

I log di navigazione rilevati dai sistemi di sicurezza vengono generati in modalità anonima per poter produrre statistiche aggregate utili ai fini di manutenzione, sviluppo e aggiornamento del sistema informatico.

Inoltre vengono anche generati log di navigazione in modalità nominativa per le verifiche di comportamenti anomali allo scopo di far cessare una o più violazioni al presente disciplinare nel rispetto dei principi di pertinenza e non eccedenza e soprattutto di gradualità dei controlli.

Tutti i log di navigazione vengono ruotati.

I log di navigazione sono conservati in copia di backup su nastro per un massimo di 35 giorni.

4.4.1.2 Cronologia delle pagine web visitate

La cronologia delle pagine web visitate è memorizzata nel profilo dei singoli lavoratori e conservata in locale sul computer utilizzato per quanto riguarda la navigazione effettuata dal computer stesso oppure conservata sul file server in rete per quanto riguarda la navigazione effettuata tramite i servizi Citrix Presentation Server. In entrambi i casi è possibile la cancellazione a carico del singolo lavoratore come da procedura contenuta nell'ALLEGATO F - ISTRUZIONI OPERATIVE PER LA CANCELLAZIONE DELLA CRONOLOGIA DELLE PAGINE WEB VISITATE al presente disciplinare.

4.4.1.3 Memoria cache delle pagine web visitate

La memoria cache delle pagine web visitate è memorizzata nel profilo dei singoli lavoratori e conservata in locale sul computer utilizzato per quanto riguarda la navigazione effettuata dal computer stesso oppure conservata sul file server in rete per quanto riguarda la navigazione effettuata tramite i servizi Citrix Presentation Server. In entrambi i casi è possibile la cancellazione a carico del singolo lavoratore come da procedura contenuta nell'ALLEGATO G - ISTRUZIONI OPERATIVE PER LA CANCELLAZIONE DELLA MEMORIA CACHE DELLE PAGINE WEB VISITATE al presente disciplinare.

4.4.1.4 Cookies

I cd. cookies, ossia le piccole quantità di informazioni che vengono inviati dai siti visitati e conservati per migliorare la navigazione, sono memorizzati nel profilo dei singoli lavoratori e conservati in locale sul computer utilizzato per quanto riguarda la navigazione effettuata dal computer stesso oppure conservata sul file server in rete per quanto riguarda la navigazione effettuata tramite i servizi Citrix Presentation Server. In entrambi i casi è possibile la cancellazione a carico del singolo lavoratore come da procedura contenuta nell'ALLEGATO H - ISTRUZIONI OPERATIVE PER LA CANCELLAZIONE DEI COOKIES al presente disciplinare.

4.4.1.5 Policy particolari

Per i gruppi:

- Amministratori
- Consiglieri comunali
- Sindaco e Vice Sindaco
 - Questi utenti possono accedere alla Posta personale e ai social network

É stata creata una policy particolare che fa sì che per tali utenti il controllo del contenuto della navigazione (filtri) sia attivo (escluse le categorie sopra evidenziate, ovvero social network ed accesso alla mail), rimanendo allo stesso tempo soggetti a log di navigazione. In particolare questa policy viene applicata sulla base degli IP address assegnati dal DHCP ai personal computer di detti utenti (legandoli al MAC address delle schede di rete stesse) che riepiloghiamo di seguito.

- ##PC Consiglieri Casa Bondi CAST0555 10.64.4.99
- ##PC Assessori Casa Bondi CAST0628 10.64.4.86
- ##PC Assessori presso Uff Tecnico CAST0391 10.64.4.34
- ##PC Vicesindaco CAST0727 10.64.4.24
- ##PC Sindaco CAST0497 10.64.4.38
- Operatori della Polizia Municipale quali Stefano Fabbri – Comandante, Bignami Cristina e Zini Raffaella. Va però specificato che la policy è applicata, come per tutte le macchine del comune, agli Ip address di detti utenti, ovvero alle macchine PC normalmente usate da detti utenti. Qualora altri utenti, e può accedere, usassero tali postazioni di lavoro, anche la loro attività non sarà soggetta a controllo. Stante gli strumenti disponibili nell'ente oggi, non è possibile una soluzione alternativa.

É stata creata una policy particolare che fa sì che per tali utenti il controllo del contenuto della navigazione (filtri) sia attivo, ma differenziato, ovvero possono chiedere l'attivazione in white list dei siti non altrimenti accessibili e necessari per lo svolgimento della loro mansione; anch'essi rimangono soggetti a log di navigazione. In particolare questa policy viene applicata sulla base degli IP address assegnati dal DHCP ai personal computer di detti utenti (legandoli al MAC address delle schede di rete stesse) che riepiloghiamo di seguito.

1. ##PC Comandante PM CAST0587 10.64.4.52
2. ##PC Segreteria PM CAST0848 10.64.4.48

4.4.2 E-mail

I log di transito della posta elettronica comunale e dei relativi sistemi di filtraggio vengono conservati (anche su supporti di backup) al massimo per un periodo di 35 giorni.

4.4.2.1 Backup file di posta

Giornalmente ne viene effettuato il backup su nastro a rotazione settimanale. Qualora un utente abbia necessità di cancellare una e-mail indesiderata presente nel proprio database di posta onde evitare che ne venga fatto il backup e che di conseguenza venga conservata sui nastri per il periodo di tempo indicato al paragrafo 4.4.2, ha la possibilità, entro le ore 22 del giorno in cui l'e-mail è arrivata nella casella di posta oppure è stata creata, di seguire le istruzioni presenti nell'ALLEGATO L – ISTRUZIONI OPERATIVE SULLA CANCELLAZIONE DI UNA E-MAIL INDESIDERATA DAL DATABASE DI POSTA al presente disciplinare.

5 ULTERIORI NORME COMPORTAMENTALI

5.1 Custodia dotazione hardware

I beni ed i servizi informatici assegnati in dotazione al lavoratore (incluso il servizio internet e posta elettronica) sono da ritenersi a tutti gli effetti un bene di proprietà dell'Ente. Per questo motivo non sono consentiti tutti gli utilizzi di detti strumenti non correlati alle attività lavorative e non in conformità con gli scopi dell'Ente stesso.

Gli assegnatari degli apparati hardware, sono tenuti a garantire il corretto utilizzo delle apparecchiature, in particolare evitando qualsiasi danneggiamento hardware e software.

Pertanto:

- è vietato lasciare incustodite le apparecchiature fornite (anche in automobile);
- è vietato spegnere le apparecchiature in modo improprio;
- è vietato effettuare sulle apparecchiature operazioni di formattazione dell'hard disk;
- è vietato modificare le configurazioni di sistema delle macchine;
- è vietato installare programmi di qualsiasi tipo, eventuali richieste per l'installazione di nuovi software di interesse professionale vanno indirizzate al responsabile dei sistemi informativi.
- il lavoratore è tenuto a controllare che non si verifichino accessi non autorizzati al sistema informatico ed ai dati in esso contenuti attraverso il personal computer e gli altri strumenti informatici o elettronici che gli sono stati affidati; qualora dovesse lasciare incustoditi anche per un breve lasso di tempo il personal computer o gli altri strumenti informatici o elettronici che gli sono stati affidati, dovrà spegnerli o quantomeno chiudere i programmi ed i documenti aperti o disconnettersi dal sistema informatico (effettuando la procedura di logoff) oppure bloccarne l'utilizzo tramite gli opportuni comandi;
- onde evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore, ed al fine di rispettare gli obblighi imposti dalla L. 633/41 e sue successive modificazioni, non è consentito installare, utilizzare o copiare software sui personal computer o sugli altri strumenti informatici o su supporti removibili se non espressamente autorizzati dall'amministratore di sistema;
- non è consentito aprire, visualizzare o copiare file sui personal computer o sugli altri strumenti informatici o su supporti removibili se non per l'attività lavorativa o se non espressamente autorizzati dall'amministratore di sistema;
- non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- non è consentito modificare per nessun motivo la configurazione hardware o software dei personal computer o degli altri strumenti informatici o elettronici se non espressamente autorizzati dall'amministratore di sistema;
- non è consentito, neppure per necessità attinenti all'attività lavorativa e salvo autorizzazione dell'amministratore del sistema, il collegamento ai personal computer affidati al lavoratore, alla rete comunale e più in generale al sistema informatico comunale di dispositivi (come ad esempio telefoni cellulari, palmari, modem, dispositivi di memorizzazione, lettori musicali, stampanti, ecc.), di apparati (come ad esempio modem,

apparati di rete o wireless) o di personal computer che non siano di proprietà dell'Ente e che non siano quelli affidati al lavoratore stesso;

- ferme restando le attività dell'amministratore di sistema di implementazione, configurazione e gestione dei software antivirus presenti nel sistema informatico, spetta al lavoratore in ultima istanza sottoporre a verifica tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, tramite gli strumenti antivirus in dotazione.

Ogni evenienza o situazione anomala va evidenziata al responsabile dei sistemi informativi.

5.2 Sicurezza in materia di autenticazione dei lavoratori

Per l'accesso al sistema informatico, al lavoratore vengono fornite una o più credenziali di autenticazione composte da un codice di identificazione (user name) associato ad una parola chiave riservata (password).

Per l'uso delle credenziali di autenticazione il lavoratore si deve attenere alle seguenti regole:

- il lavoratore deve cambiare la parola chiave al primo accesso al sistema informatico e successivamente almeno ogni **60 giorni**; l'amministratore di sistema ha la facoltà di imporre tale cambiamento periodico;
- la parola chiave deve essere composta da almeno otto caratteri alfanumerici e deve contenere caratteri appartenenti ad almeno tre delle seguenti categorie:
 - lettere maiuscole,
 - lettere minuscole,
 - numeri,
 - caratteri speciali (punteggiatura, lettere accentate, parentesi, ...)
- la parola chiave deve formare un codice non banale che non abbia alcun riferimento con dati personali (user name, nome, cognome, indirizzo, data di nascita....) del lavoratore, di parenti, amici, colleghi o conoscenti;
- la parola chiave deve essere mantenuta segreta e non deve essere rivelata ad alcuno; essa può essere conservata in forma scritta esclusivamente se custodita con diligenza affinché solo il lavoratore stesso possa accedervi.

5.3 Modalità di memorizzazione di documenti sui sistemi comunali

Per il salvataggio dei dati, l'uso delle unità di rete e dei supporti di memorizzazione, il lavoratore si deve attenere alle seguenti regole:

- le unità di rete sono aree di condivisione di informazioni strettamente lavorative e non possono in alcun modo essere utilizzate per scopi diversi; pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità;
- il lavoratore può conservare quantità modeste di documenti e dati non inerenti l'attività lavorativa solamente sul disco locale del personal computer in dotazione (e non sulle unità di rete); tali documenti non sono sottoposti a backup: il lavoratore, se nel proprio interesse, è tenuto a provvedere autonomamente ad eseguirne copia periodica; inoltre si segnala che tali documenti potrebbero essere visualizzati da altri lavoratori che dovessero utilizzare lo stesso personal computer: il lavoratore, se nel proprio interesse, è tenuto a non conservare

sul personal computer in dotazione documenti o dati che ritenesse non opportuno venissero a conoscenza di altri; in ogni caso è fatto divieto assoluto di memorizzare e conservare documenti, files o dati ottenuti in modo illegale (ad esempio software soggetti a copyright, file musicali soggetti a copyright, file video soggetti a copyright, ecc...);

- è in generale da evitare il salvataggio di dati personali riferiti all'attività lavorativa sui singoli personal computer o su altri strumenti informatici o elettronici; i dati personali devono essere salvati di norma sulle unità di rete predisposte dall'amministratore di sistema;
- non è assolutamente consentito il salvataggio di **dati sensibili e/o giudiziari** sui singoli personal computer o su altri strumenti informatici o elettronici; i dati sensibili e/o giudiziari, anche allo scopo di ottemperare agli obblighi di back-up e disaster recovery per il ripristino di tali dati previsto dalla normativa in materia, devono essere salvati unicamente nelle apposite unità di rete predisposte dall'amministratore di sistema; l'elenco delle unità di rete a disposizione dei lavoratori è contenuto nell'ALLEGATO M - UNITÀ DI RETE al presente disciplinare;
- qualora, per motivi di necessità, sia necessario conservare dati personali inerenti l'attività lavorativa sui singoli personal computer o su altri strumenti informatici o elettronici, i lavoratori hanno l'obbligo di provvedere con cadenza almeno settimanale ad effettuare una copia di detti dati su supporti rimovibili secondo le indicazioni contenute nelle lettere di incarico; l'utilizzo, la conservazione e l'eventuale distruzione di detti supporti rimovibili devono essere effettuati da parte dei lavoratori secondo le indicazioni contenute nelle lettere di incarico;
- non è consentito, di norma, l'utilizzo di supporti rimovibili per la memorizzazione di dati ed in particolar modo di dati sensibili e/o giudiziari; eventuali utilizzi, per motivi di necessità, di supporti rimovibili per la memorizzazione di **dati sensibili e/o giudiziari** da parte dei lavoratori sono permessi unicamente per gli usi consentiti dalle rispettive lettere di incarico; l'utilizzo, la conservazione e l'eventuale distruzione di detti supporti rimovibili devono essere effettuati da parte dei lavoratori secondo le indicazioni contenute nelle lettere di incarico; al termine del trattamento i supporti rimovibili contenenti **dati sensibili e/o giudiziari** dovranno essere cancellati ove possibile oppure distrutti o resi inutilizzabili al fine di rendere non intelligibili e tecnicamente non ricostruibili le informazioni in essi contenute;
- in caso di utilizzo di strumenti informatici o elettronici (ad esempio stampanti, fax o fotocopiatrici) per riprodurre copie su carta di dati personali, sensibili o giudiziari, il lavoratore è tenuto a non lasciare tali copie nei pressi di detti strumenti o comunque in luoghi accessibili a persone non incaricate al trattamento; qualora tali copie o anche altri documenti contenenti dati personali, dati sensibili e/o giudiziari, non fossero più necessari per l'attività lavorativa il lavoratore è tenuto a riporle negli appositi raccoglitori per la distruzione, avendo cura di renderli inintelligibili ed inutilizzabili.

5.4 Installazione software

Tutti i programmi installati sui dispositivi in uso agli utilizzatori, sono stati testati e validati dai Sistemi Informativi del Comune. Onde evitare problemi di malfunzionamento, sicurezza e instabilità dei sistemi, è fatto divieto assoluto di installazione di qualsiasi software / utility / programma da parte degli utilizzatori.

Nel caso in cui si ritenesse di avere necessità di un software / utility / programma non installato sul PC in dotazione, è necessario contattare il responsabile dei sistemi informativi per valutare assieme l'effettiva opportunità di installazione dell'applicativo stesso.

Il sistema operativo e tutti i moduli e programmi software messi a disposizione devono essere utilizzati esclusivamente per attività professionali; al contrario non possono essere utilizzati per attività profittevoli, e non possono essere copiati e distribuiti su installazioni esterne.

E' fatto divieto assoluto dell'utilizzo e/o possesso di software illegalmente copiato.

5.5 Attività dell'amministratore di sistema

Per i soli fini di amministrazione, gestione e manutenzione del sistema informatico, l'amministratore di sistema ha la possibilità di utilizzare oppure di connettersi da remoto alle risorse disponibili su ciascun personal computer in dotazione ai lavoratori e più in generale a ciascun dispositivo connesso alla infrastruttura informatica.

L'amministratore di sistema provvede ad implementare, configurare e gestire uno o più software antivirus in grado di proteggere l'infrastruttura informatica da virus e più in generale da malware (un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito). Tali software antivirus, in base alle configurazioni effettuate dall'amministratore di sistema, sono in grado automaticamente di rilevare le infezioni da virus informatici e di riparare, mettere in quarantena o eventualmente eliminare i file infetti.

In previsione della possibilità che in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba accedere a dati accessibili solamente con le credenziali di autenticazione di un lavoratore, ciascun lavoratore, inviando richiesta scritta ai responsabili del trattamento, può delegare un altro lavoratore a rendere disponibili al titolare o ai responsabili i dati necessari per lo svolgimento dell'attività lavorativa, su richiesta del titolare o dei responsabili. Qualora tale delega non sia stata espressa, le predette operazioni sono effettuate dall'amministratore di sistema, sempre su richiesta del titolare o dei responsabili. A cura del titolare del trattamento, di tale attività viene redatto apposito verbale e viene informato il lavoratore tramite posta elettronica oppure, qualora non possibile, mediante comunicazione scritta.

Per i soli fini di amministrazione, gestione e manutenzione del sistema informatico, l'amministratore di sistema ha la possibilità di accedere a tutti i dati presenti nel sistema informatico stesso compresi tutti i file conservati nei dischi di rete, nei dischi dei personal computer e negli altri dispositivi connessi.

L'amministratore di sistema ha la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione del presente documento, dandone contestuale comunicazione al lavoratore interessato, ove ciò sia possibile.

All'amministratore di sistema e più in generale ai Servizi Informatici è consentito l'uso di supporti rimovibili per le operazioni di backup dei dati. Le modalità di realizzazione, utilizzo, conservazione e

distruzione dei dati di backup sono specificate nelle lettere di incarico per gli amministratori di sistema.

6 MODALITÀ DEI CONTROLLI

Nel rispetto delle leggi vigenti e dei provvedimenti che vietano il trattamento effettuato mediante sistemi *hardware* e *software* preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire sistematicamente l'attività dei lavoratori, il Comune di Castenaso può procedere a controlli finalizzati alla sicurezza, all'efficienza e all'organizzazione dei sistemi e delle strutture, i quali possono riguardare incidentalmente anche informazioni personali dei lavoratori.

Le modalità di tali controlli sono di seguito illustrate.

6.1 Internet

Periodicamente il Comune di Castenaso genera **report statistici in forma anonima** ed aggregata (per esempio in base a gruppi di utenti, categorie di siti web, frequenze di navigazione, etc.) relativi al traffico Internet.

Possibilità statistiche:

- Statistiche/analisi sui siti leciti
- Statistiche/analisi sui siti bloccati
- Statistiche/analisi sui siti non categorizzati

Nel caso in cui a seguito di controlli, effettuati sempre e comunque in forma anonima, risultasse rilevante evidenza di un sospetto utilizzo illegale o non consentito della navigazione web, si attiverà la seguente procedura:

- L'Amministratore di Sistema segnala via e-mail o comunque per iscritto l'anomalia al proprio Dirigente di riferimento.
- Contestualmente l'Amministratore di Sistema effettua una copia su supporto informatico non cancellabile da conservare in luogo sicuro, **dei log anonimi e dei log ip da cui risulti il sospetto** illecito che sono stati generati dal sistema informatico come indicato al paragrafo 4.4.1.1.
- Il Dirigente effettua una comunicazione all'interno del Comune dell'evento con indicazione della tipologia di illecito e relativo invito alla cessazione dell'attività illegale o non consentita.
- Il Dirigente se lo ritiene opportuno richiede via e-mail o comunque per iscritto all'Amministratore di Sistema una successiva verifica periodica finalizzata all'individuazione di un eventuale riverificarsi della medesima attività.
- Solo nel caso in cui a seguito di tali controlli suddetti risulti il perdurare dell'attività, l'Amministratore di Sistema ne darà comunicazione via e-mail o comunque per iscritto al Dirigente il quale potrà richiedere l'individuazione dell'autore del comportamento illecito e la relativa applicazione delle procedure disciplinari tramite l'utilizzo dei log conservati su supporto informatico come indicato precedentemente.
- Qualora il Dirigente ritenga conclusa la procedura provvederà a richiedere via e-mail o comunque per iscritto all'Amministratore di Sistema la distruzione dei supporti contenenti i log.

6.2 E-mail

Periodicamente il Comune di Castenaso genera report statistici in forma anonima ed aggregata (per esempio in base a gruppi di utenti, domini di destinazione delle mail, domini di provenienza delle mail, frequenza di invio/ricezione, etc.) relativi al traffico di Posta Elettronica.

Possibilità statistiche:

- Statistiche/analisi sulle e-mail inviate / ricevute
- Statistiche/analisi sulle e-mail bloccate

Nel caso in cui a seguito di controlli, effettuati sempre e comunque in forma anonima, risultasse un sospetto utilizzo illegale o non consentito dello strumento di posta elettronica si attiverà la seguente procedura:

- L'Amministratore di Sistema segnala via e-mail o comunque per iscritto l'anomalia al proprio Dirigente di riferimento.
- Contestualmente l'Amministratore di Sistema effettua una copia su supporto informatico non cancellabile da conservare in luogo sicuro, dei log da cui risulti il sospetto illecito che sono stati generati dal sistema informatico.
- Il Dirigente effettua una comunicazione all'interno del Comune dell'evento con indicazione della tipologia di illecito e relativo invito alla cessazione dell'attività illegale o non consentita.
- Il Dirigente se lo ritiene opportuno richiede via e-mail o comunque per iscritto all'Amministratore di Sistema una successiva verifica periodica finalizzata all'individuazione di un eventuale riverificarsi della medesima attività.
- Solo nel caso in cui a seguito di tali controlli suddetti risulti il perdurare dell'attività, l'Amministratore di Sistema ne darà comunicazione via e-mail o comunque per iscritto al Dirigente il quale potrà richiedere l'individuazione dell'autore del comportamento illecito e la relativa applicazione delle procedure disciplinari tramite l'utilizzo dei log conservati su supporto informatico come indicato precedentemente.
- Qualora il Dirigente ritenga conclusa la procedura provvederà a richiedere via e-mail o comunque per iscritto all'Amministratore di Sistema la distruzione dei supporti contenenti i log.

6.3 File system

Il Comune di Castenaso per motivi di sicurezza e di manutenzione del sistema, più specificatamente per la risoluzione di problemi, si riserva la possibilità di effettuare dei controlli, individuando le operazioni (salvataggio, eliminazione, modifica, etc.) effettuate dai lavoratori sui file contenuti nei dischi di rete, nei dischi dei personal computer e negli altri dispositivi connessi

7 PROCEDURE IN CASO DI CESSAZIONE DEL RAPPORTO LAVORATIVO

In caso di cessazione del rapporto lavorativo, si applicano le seguenti procedure:

7.1 Documenti memorizzati sui sistemi comunali

I documenti informatici prodotti dal lavoratore nell'esercizio dell'attività professionale a favore del Comune di Castenaso e doverosamente inseriti nei sistemi informativi comunali restano nella piena ed esclusiva disponibilità del Comune. Salvo esplicita autorizzazione scritta da parte del Comune di Castenaso, il lavoratore non può formare o ottenere copia dei predetti documenti né farne alcun uso dopo la cessazione del rapporto di lavoro.

I documenti non attinenti l'attività lavorativa conservati dal lavoratore all'interno dei dischi del personal computer in dotazione devono essere eliminati a cura del lavoratore medesimo, previa eventuale copia. In caso contrario, il Comune di Castenaso provvederà direttamente all'eliminazione, a rapporto lavorativo cessato. Tali documenti possono essere conservati ed utilizzati a fini personali dal lavoratore, purché non riguardino in nessun modo l'attività professionale cessata.

7.2 E-mail

Le e-mail relative ad ogni account di posta elettronica comunale NON NOMINATIVO restano nella piena ed esclusiva disponibilità del Comune di Castenaso; salvo esplicita autorizzazione scritta da parte del Comune di Castenaso, il lavoratore non può formare o ottenere copia delle predette e-mail né farne alcun uso dopo la cessazione del rapporto di lavoro.

Le e-mail relative all'account di posta elettronica comunale NOMINATIVO PROF restano nella piena disponibilità del Comune. Trattandosi tuttavia di corrispondenza formatasi in relazione ad un account e-mail nominativo, il lavoratore può chiedere copia delle e-mail e conservarle a fini esclusivamente personali, con esclusione di ogni diverso utilizzo dopo la cessazione del rapporto di lavoro. Il lavoratore può comunque chiedere ed ottenere di eliminare dai sistemi comunali eventuali e-mail di carattere strettamente personale, previa eventuale copia personale.

7.3 Tracce elettroniche ("log")

I log, ossia le tracce elettroniche relative all'utilizzo di strumenti elettronici da parte del lavoratore, tracciati dai sistemi comunali per ragioni tecniche, produttive, organizzative, di sicurezza (log di navigazione, log di accesso a sistemi o applicazioni, ecc.) sono conservati per il tempo strettamente necessario alle finalità perseguite caso per caso, come indicato in dettaglio nelle precedenti Sezioni del presente disciplinare.

8 SANZIONI APPLICABILI E RELATIVE PROCEDURE

Il Comune di Castenaso è consapevole e condivide che:

- nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata;
- l'eventuale controllo è perciò lecito solo se sono rispettati i principi di pertinenza e non eccedenza, e soprattutto di gradualità dei controlli;
- nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il Comune può nondimeno adottare misure che consentano la verifica di comportamenti anomali, sia pure preferendo un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree;
- il controllo anonimo si conclude, in prima battuta e di regola, con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti comunali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite;
- va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

Tuttavia, controlli su dati aggregati e/o anonimi possono talora rivelarsi insufficienti o inadeguati allo scopo di far cessare una o più violazioni al presente disciplinare. In tal caso può essere necessario individuare personalmente il lavoratore che ha assunto un comportamento in violazione del presente disciplinare e, come *extrema ratio* (principio di gradualità), potrà attivarsi la procedura di cui al capo V del CCNL 6.7.1995 del comparto Regioni Autonomie Locali , tenuto conto che in relazione alla gravità dell'infrazione si applicano le seguenti sanzioni:

- rimprovero verbale
- rimprovero scritto (censura)
- multa di importo fino a 4 ore di retribuzione
- sospensione dal servizio e dalla retribuzione fino a 10 gg.
- sospensione dal servizio con privazione della retribuzione da 11 gg. a 6 mesi
- licenziamento con preavviso
- licenziamento senza preavviso

Il tipo e l'entità di ciascuna delle sanzioni sono determinate in relazione ai seguenti criteri generali previsti dal CCNL, nel rispetto delle procedure dallo stesso fissate:

- intenzionalità del comportamento, grado di negligenza, imprudenza o imperizia dimostrate, tenuto conto anche della prevedibilità dell'evento,
- rilevanza degli obblighi violati,
- responsabilità connesse alla posizione di lavoro occupata dal dipendente,
- grado di danno o di pericolo causato all'ente, agli utenti o a terzi ovvero al disservizio determinatosi,

- sussistenza di circostanze aggravanti o attenuanti, con particolare riguardo al comportamento del lavoratore, ai precedenti disciplinari nell'ambito del biennio previsto dalla legge, al comportamento verso gli utenti,
- al concorso nella mancanza di più lavoratori in accordo tra loro,
- la recidiva nelle mancanze, già sanzionate nel biennio di riferimento, comporta una sanzione di maggiore gravità tra quelle previste.

9 ALLEGATO A - ELENCO DEGLI STRUMENTI SOFTWARE UTILIZZATI PER L'ATTIVITÀ DI ASSISTENZA TECNICA INFORMATICA

Gli strumenti software utilizzati dagli amministratori di sistema per svolgere l'attività di assistenza tecnica informatica sono i seguenti:

- software UltraVNC per l'accesso al desktop utente ed alle relative sessioni di lavoro sui personal computer in dotazione ai lavoratori,
- funzionalità di shadowing per l'accesso agli applicativi in uso ed alle relative sessioni di lavoro sull'infrastruttura Citrix Presentation Server.

10 ALLEGATO B - ELENCO DEI PROGRAMMI A DISPOSIZIONE PER LA NAVIGAZIONE IN INTERNET E PER LA POSTA ELETTRONICA

10.1 NAVIGAZIONE IN INTERNET

- Microsoft Internet Explorer
- Mozilla Firefox 3.5.5

10.2 POSTA ELETTRONICA

- IBM Lotus Notes
-

11 ALLEGATO C - CATEGORIE DI FILTRAGGIO DEI SITI WEB

- adult
- antispware
- chat
- dialers
- filehosting
- gambling
- hacking
- instantmessaging
- mail
- mixed_adult
- onlineauctions
- onlinegames
- onlinepayment
- personalfinance
- phishing
- porn
- proxy
- radio
- sexuality
- socialnetworking
- spyware
- virusinfected
- warez
- webmail

12 ALLEGATO D - ELENCO DELLE TIPOLOGIE DI FILE BLOCCATI IN DOWNLOAD DA INTERNET

12.1 ESTENSIONI DI FILE

- .ade	- .hto	- .ogm	- .wma
- .adp	- .img	- .ops	- .wmd
- .aif	- .inf	- .otf	- .wmf
- .aifc	- .ini	- .pcd	- .wms
- .aiff	- .ins	- .pif	- .wmv
- .app	- .iso	- .pls	- .wmx
- .asd	- .isp	- .po1	- .wmz
- .asf	- .jse	- .prf	- .wsc
- .asr	- .lib	- .prg	- .wsf
- .asx	- .lnk	- .qt	- .wsh
- .au	- .lsf	- .ra	- .wvx
- .avi	- .lsx	- .ram	
- .bas	- .m3u	- .rar	
- .bat	- .m4u	- .reg	
- .bin	- .mda	- .rm	
- .bz2	- .mdb	- .rmi	
- .c2d	- .mde	- .scf	
- .cab	- .mdt	- .scr	
- .cd	- .mdw	- .sct	
- .cdr	- .mdz	- .sea	
- .chm	- .mid	- .sh	
- .cif	- .mov	- .shb	
- .cmd	- .movie	- .shs	
- .com	- .mp2	- .sit	
- .cpl	- .mp3	- .smi	
- .crt	- .mp4	- .snd	
- .cue	- .mpa	- .sub	
- .dat	- .mpe	- .sys	
- .dll	- .mpeg	- .tar	
- .dmg	- .mpg	- .tgz	
- .exe	- .mpv2	- .url	
- .fcd	- .msc	- .vb	
- .flv	- .msi	- .vbe	
- .fxp	- .msp	- .vbs	
- .gcd	- .mst	- .vcs	
- .gz	- .nrg	- .vxd	
- .hlp	- .nsc	- .wav	
- .hqx	- .ocx	- .wax	
- .hta	- .ogg	- .wm	

12.2 TIPOLOGIE MIME

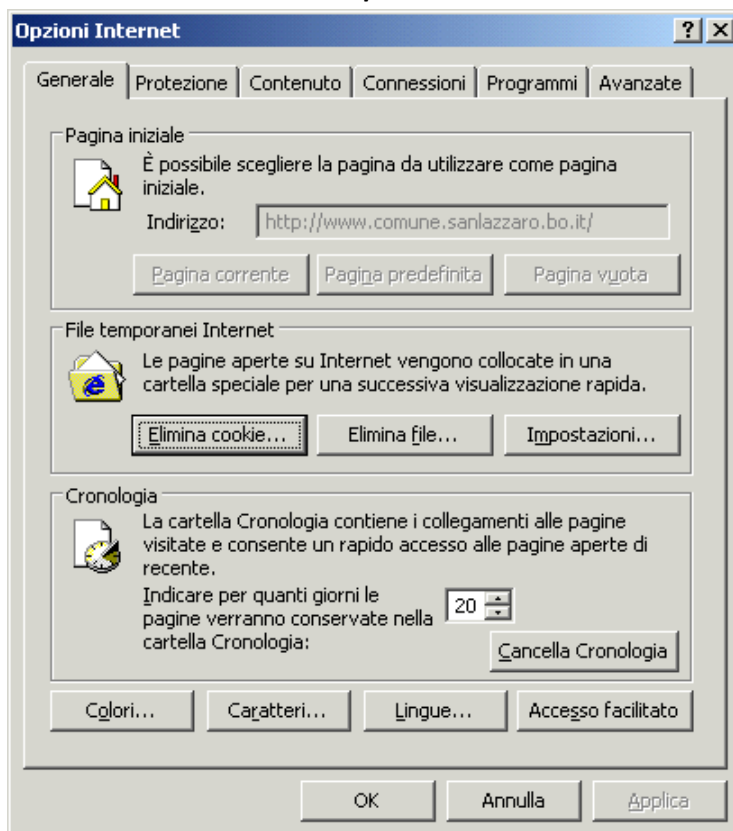
- audio/mpeg
- audio/x-mpegurl
- audio/x-mpeg
- audio/x-pn-realaudio
- audio/x-realaudio
- audio/x-wav
- audio/x-ms-wma
- audio/x-ms-wax
- audio/x-scpls
- video/mpeg
- video/x-mpeg2
- video/acorn-replay
- video/quicktime
- video/x-msvideo
- video/msvideo
- video/x-ms-asf
- video/x-ms-wmv
- video/x-ms-wvx
- video/x-ms-wm
- video/x-flv
- application/gzip
- application/x-gzip
- application/zip
- application/compress
- application/x-compress
- application/java-vm
- application/vnd.ms-asf
- application/vnd.ms.wms-hdr.asfv1
- application/x-mms-framed
- application/x-ms-wmd
- application/x-ms-wmz
- application/vnd.rn-realmedia
- application/ogg
- application/octet-stream

13 ALLEGATO E - ELENCO DELLE ESTENSIONI DI FILE BLOCCATI COME ALLEGATI ALLE E-MAIL

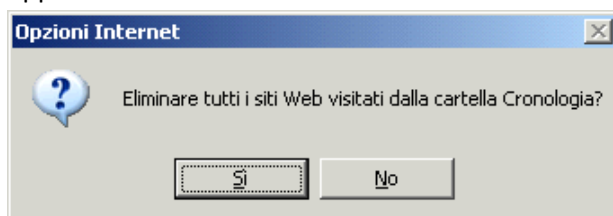
- .ade	- .inf	- .pif	- .wmz
- .adp	- .ini	- .pls	- .wsc
- .aif	- .ins	- .po1	- .wsf
- .aifc	- .iso	- .prf	- .wsh
- .aiff	- .isp	- .prg	- .wvx
- .app	- .jse	- .qt	
- .asd	- .lib	- .ra	
- .asf	- .lnk	- .ram	
- .asr	- .lsf	- .rar	
- .asx	- .lsx	- .reg	
- .au	- .m3u	- .rm	
- .avi	- .m4u	- .rmi	
- .bas	- .mda	- .scf	
- .bat	- .mdb	- .scr	
- .bin	- .mde	- .sct	
- .bz2	- .mdt	- .sea	
- .c2d	- .mdw	- .sh	
- .cab	- .mdz	- .shb	
- .cd	- .mid	- .shs	
- .cdr	- .mov	- .sit	
- .chm	- .movie	- .smi	
- .cif	- .mp2	- .snd	
- .cmd	- .mp3	- .sub	
- .com	- .mp4	- .sys	
- .cpl	- .mpa	- .tar	
- .crt	- .mpe	- .tgz	
- .cue	- .mpeg	- .url	
- .dat	- .mpg	- .vb	
- .dll	- .mpv2	- .vbe	
- .dmg	- .msc	- .vbs	
- .exe	- .msi	- .vcs	
- .fcd	- .msp	- .vxd	
- .flv	- .mst	- .wav	
- .fxp	- .nrg	- .wax	
- .gcd	- .nsc	- .wm	
- .gz	- .ocx	- .wma	
- .hlp	- .ogg	- .wmd	
- .hqx	- .ogm	- .wmf	
- .hta	- .ops	- .wms	
- .hto	- .otf	- .wmv	
- .img	- .pcd	- .wmx	

14 ALLEGATO F - ISTRUZIONI OPERATIVE PER LA CANCELLAZIONE DELLA CRONOLOGIA DELLE PAGINE WEB VISITATE

1. Cliccare sul pulsante **Strumenti – Opzioni Internet**.
2. Verrà visualizzata la finestra **Opzioni Internet**.



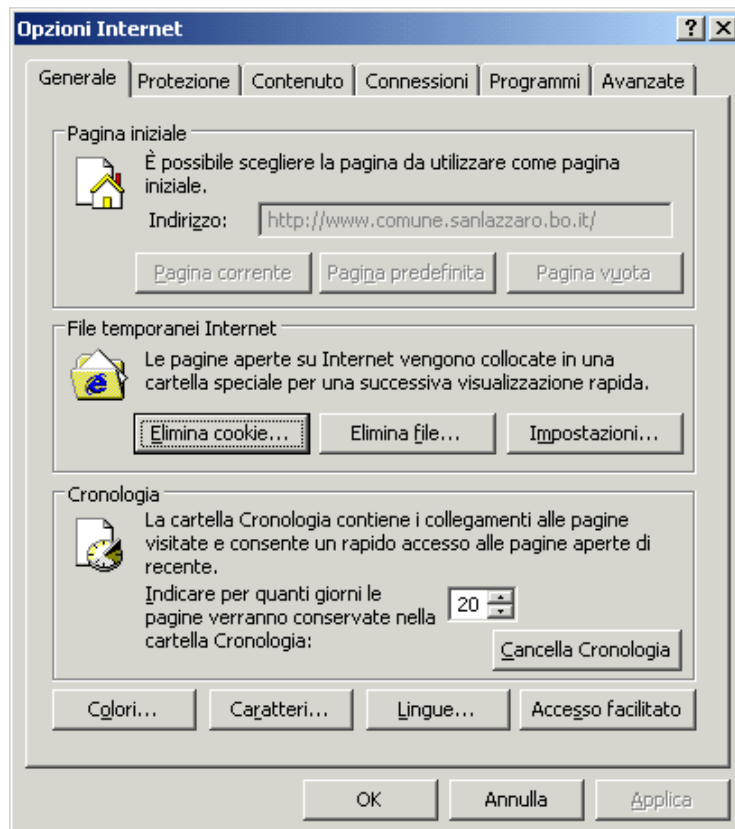
3. Cliccare sul pulsante **Cancella Cronologia**.
4. Apparirà una finestra di richiesta di conferma:



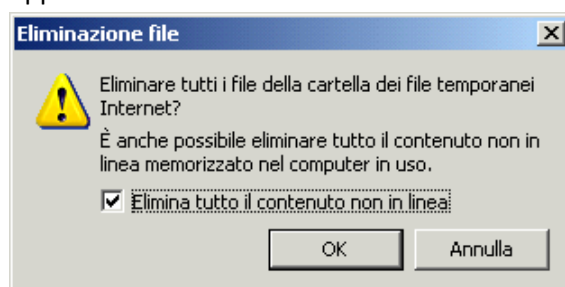
5. Cliccare sul pulsante **Sì**.
6. Nella finestra Opzioni Internet cliccare sul pulsante **Ok**.

15 ALLEGATO G - ISTRUZIONI OPERATIVE PER LA CANCELLAZIONE DELLA MEMORIA CACHE DELLE PAGINE WEB VISITATE

1. Cliccare sul pulsante **Strumenti – Opzioni Internet**.
2. Verrà visualizzata la finestra **Opzioni Internet**.



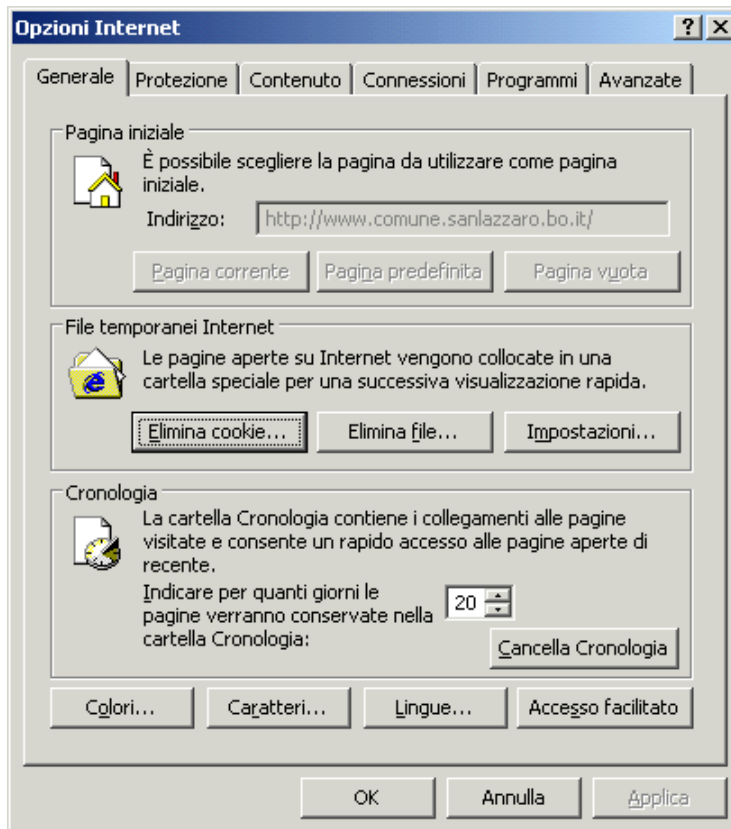
3. Cliccare sul pulsante **Elimina file**.
4. Apparirà una finestra di richiesta di conferma:



5. Attivare l'opzione **Elimina tutto il contenuto non in linea**.
6. Cliccare sul pulsante **Ok**.
7. Nella finestra Opzioni Internet cliccare sul pulsante **Ok**.

16 ALLEGATO H - ISTRUZIONI OPERATIVE PER LA CANCELLAZIONE DEI COOKIES

1. Cliccare sul pulsante **Strumenti – Opzioni Internet**.
2. Verrà visualizzata la finestra **Opzioni Internet**.



3. Cliccare sul pulsante **Elimina cookie**.
4. Apparirà una finestra di richiesta di conferma:



5. Cliccare sul pulsante **Ok**.
6. Nella finestra Opzioni Internet cliccare sul pulsante **Ok**.

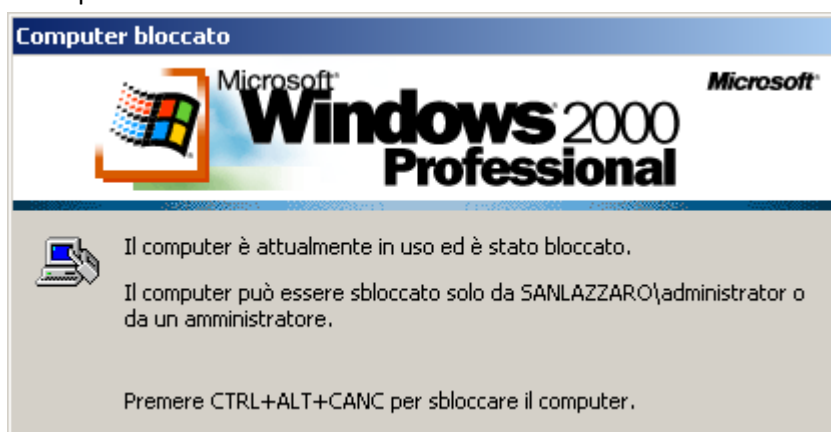
17 ALLEGATO I - ISTRUZIONI OPERATIVE SU COME BLOCCARE IL COMPUTER

17.1 Blocco del computer

1. Premere contemporaneamente i tasti **CTRL-ALT-CANC**.
2. Apparirà la finestra **Protezione di Windows**:



3. Cliccare sul pulsante **Blocca computer**.
4. Il computer è bloccato:



17.2 Sblocco del computer

1. Per sbloccare il computer, premere contemporaneamente i tasti **CTRL-ALT-CANC**.
2. Apparirà la finestra **Sblocco computer**:



3. Nel campo **Nome utente** digitare lo user name.
Nel campo **Password** digitare la password.
Cliccare sul pulsante **Ok**.

18 ALLEGATO J - ISTRUZIONI OPERATIVE SULL'UTILIZZO DEL SOFTWARE ANTIVIRUS

L'antivirus è in funzione quando è presente l'icona sulla barra delle applicazioni: 

1. Andando con il mouse sull'icona dell'antivirus e attendendo qualche istante è possibile vedere la versione dei **pattern** (le informazioni sui virus) e la versione dell'**engine** (il motore di scansione):

OfficeScan (Online) Antivirus Eng/Ptn: 9.100.1001/6.913.00 DCS Eng/Ptn: 6.2.1016/1072



2. Il menù dell'antivirus si visualizza cliccando con il tasto destro sull'icona dell'antivirus:

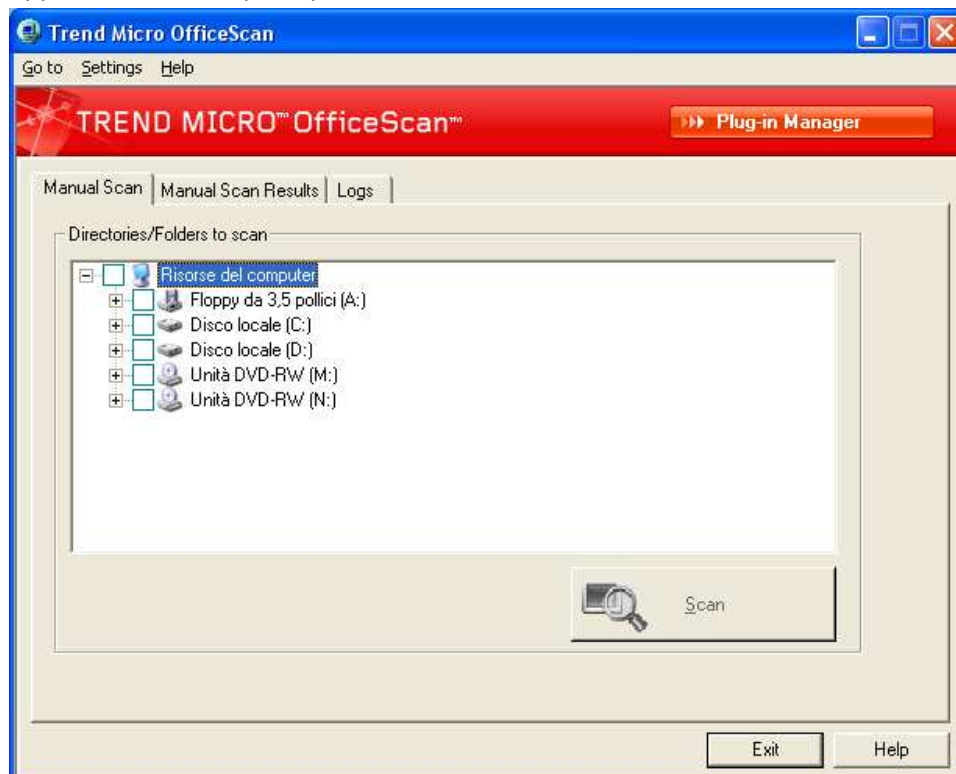
OfficeScan Console
Component Versions Update Now
Enable Roaming Mode Disable Scheduled Update
Scheduled Scan Advanced Settings
Plug-in Manager
Unload OfficeScan

3. Per effettuare una scansione selezionare la voce **OfficeScan Main** dal menù dell'antivirus:

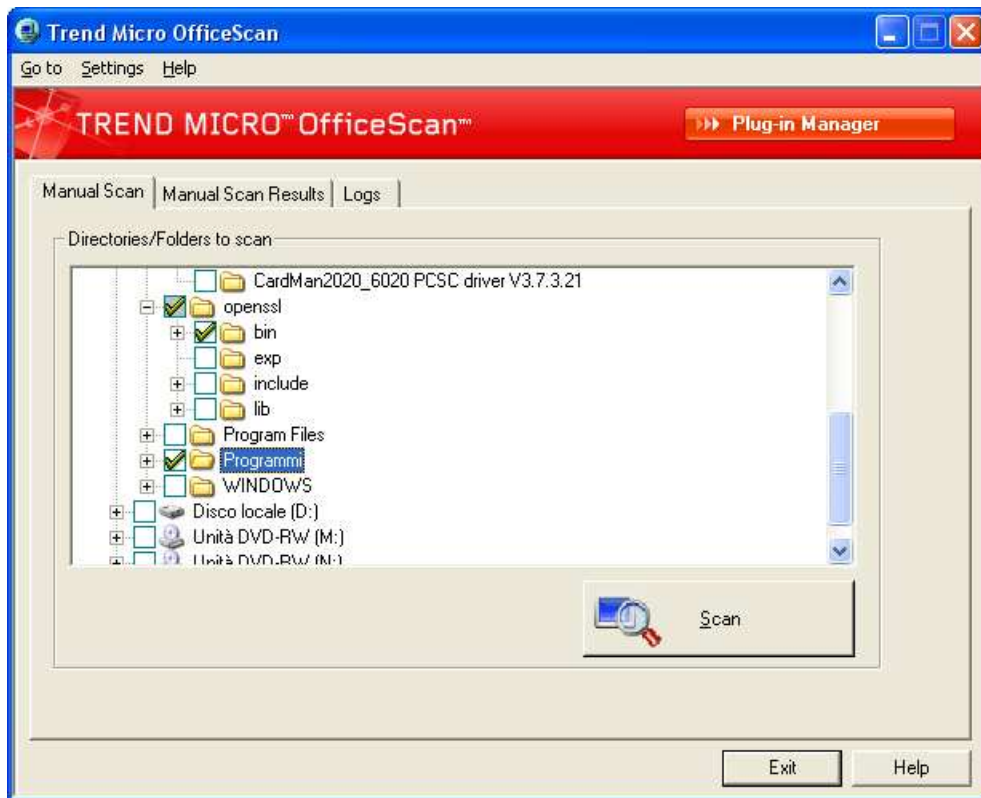
OfficeScan Console
Component Versions Update Now
Enable Roaming Mode Disable Scheduled Update
Scheduled Scan Advanced Settings
Plug-in Manager
Unload OfficeScan



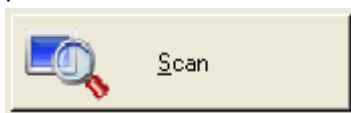
4. Apparirà la finestra principale dell'antivirus:



5. E' possibile scegliere se fare la scansione dell'intero computer, di un solo disco (anche di un dischetto floppy), di un insieme di cartelle oppure di un insieme di file.



6. Una volta effettuata la selezione di quello su cui effettuare la scansione, cliccare sul pulsante **Scan**:



7. Attendere il termine della scansione:



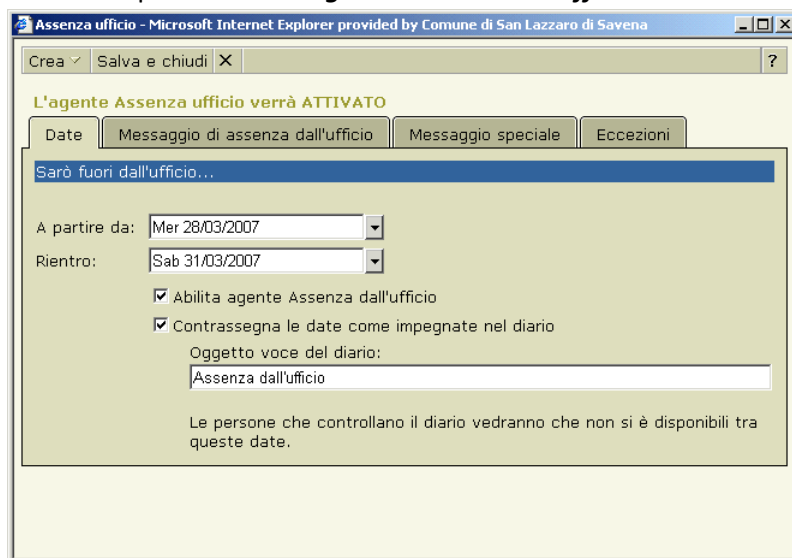
19 ALLEGATO K - ISTRUZIONI OPERATIVE SULL'UTILIZZO DEL MESSAGGIO DI ASSENZA DALL'UFFICIO

19.1 Lotus iNotes

1. Cliccare sul pulsante **Strumenti – Assenza ufficio**:



2. Verrà visualizzata la finestra **Assenza ufficio**.
3. Nella scheda **Date** impostare la data di inizio e la data di fine del periodo in cui attivare la funzionalità di assenza dall'ufficio.
4. Attivare l'opzione **Abilita agente Assenza dall'ufficio**.



5. Nella scheda **Messaggio di assenza dall'ufficio** specificare l'oggetto ed il testo del messaggio che verrà inviato nel periodo di assenza dall'ufficio.

The screenshot shows a web browser window titled 'Assenza ufficio - Microsoft Internet Explorer provided by Comune di San Lazzaro di Savena'. The page has a navigation bar with 'Crea' (selected), 'Salva e chiudi', and a help icon. Below the navigation bar, a status message reads 'L'agente Assenza ufficio verrà ATTIVATO'. There are four tabs: 'Date', 'Messaggio di assenza dall'ufficio' (selected), 'Messaggio speciale', and 'Eccezioni'. A text box explains: 'Questo è il messaggio standard inviato mentre si è assenti dall'ufficio. Per specificare un messaggio speciale per la risposta ad alcune persone specifiche, utilizzare il pannello "Messaggio speciale".' The form contains the following fields: 'Per:' with the value 'Chiunque', 'Oggetto:' with the value 'Mario Rossi è assente dall'ufficio.', a date range 'Sarò assente dall'ufficio a partire da Mer 28/03/2007 fino a Sab 31/03/2007.', and a large text area with the value 'Risponderò al messaggio al mio ritorno.'

6. Nella scheda **Messaggio speciale** eventualmente specificare se inviare ad alcuni destinatari un messaggio speciale di assenza dall'ufficio. Specificare i destinatari, l'oggetto ed il testo del messaggio speciale.

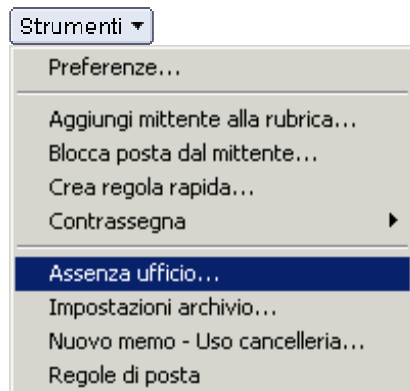
The screenshot shows the same web browser window, but with the 'Messaggio speciale' tab selected. A text box explains: 'Il messaggio viene inviato solo quando si riceve posta dalle persone elencate sotto.' The form contains the following fields: 'Per:' with a dropdown menu showing 'Claudio Bianchi', 'Oggetto:' with the value 'Mario Rossi è assente dall'ufficio.', a date range 'Sarò assente dall'ufficio a partire da Mer 28/03/2007 fino a Sab 31/03/2007.', and a large text area with the value 'Finisci tu il lavoro.'

7. Nella scheda **Eccezioni** eventualmente specificare eventuali eccezioni all'invio del messaggio di assenza dall'ufficio.

8. Cliccare sul pulsante **Salva e chiudi**.

19.2 Lotus Notes

1. Cliccare sul pulsante **Strumenti – Assenza ufficio**:



2. Verrà visualizzata la finestra **Assenza ufficio**.
3. Nella scheda **Date** impostare la data di inizio e la data di fine del periodo in cui attivare la funzionalità di assenza dall'ufficio.



4. Nella scheda **Messaggio di assenza dall'ufficio** specificare l'oggetto ed il testo del messaggio che verrà inviato nel periodo di assenza dall'ufficio.

The screenshot shows a window titled "Assenza ufficio" with a status bar indicating "Disabilitato". Below the status bar, there is a text area explaining that Notes can respond automatically to incoming mail when the user is not in the office. A tabbed interface at the top shows three tabs: "Date", "Messaggio di assenza dall'ufficio" (which is selected), and "Messaggio speci...". The main area contains a form for a predefined absence message. The "Per:" field is set to "Chiunque". The "Oggetto:" field contains the text "mario Rossi è assente dall'ufficio.". Below this, there is a text area with the message: "Sarò assente dall'ufficio a partire da 28/03/2007 e non tornerò fino al 31/03/2007. Risponderò al messaggio al mio ritorno." At the bottom of the window are three buttons: "OK", "Annulla", and "Abilita".

5. Nella scheda **Messaggio speciale** eventualmente specificare se inviare ad alcuni destinatari un messaggio speciale di assenza dall'ufficio. Specificare i destinatari, l'oggetto ed il testo del messaggio speciale.

The screenshot shows the same "Assenza ufficio" window, but with the "Messaggio speciale" tab selected. The status bar remains "Disabilitato". The text area explains that the message will only be sent when receiving mail from the listed recipients. The form fields are: "Per:" with a dropdown menu showing "Claudio Bianchi"; "Oggetto:" with the text "mario Rossi è assente dall'ufficio."; and a text area with the message: "Sarò assente dall'ufficio a partire da 28/03/2007 e non tornerò fino al 31/03/2007. Finisci tu il lavoro." The "OK", "Annulla", and "Abilita" buttons are at the bottom.

6. Nella scheda **Eccezioni** eventualmente specificare eventuali eccezioni all'invio del messaggio di assenza dall'ufficio.

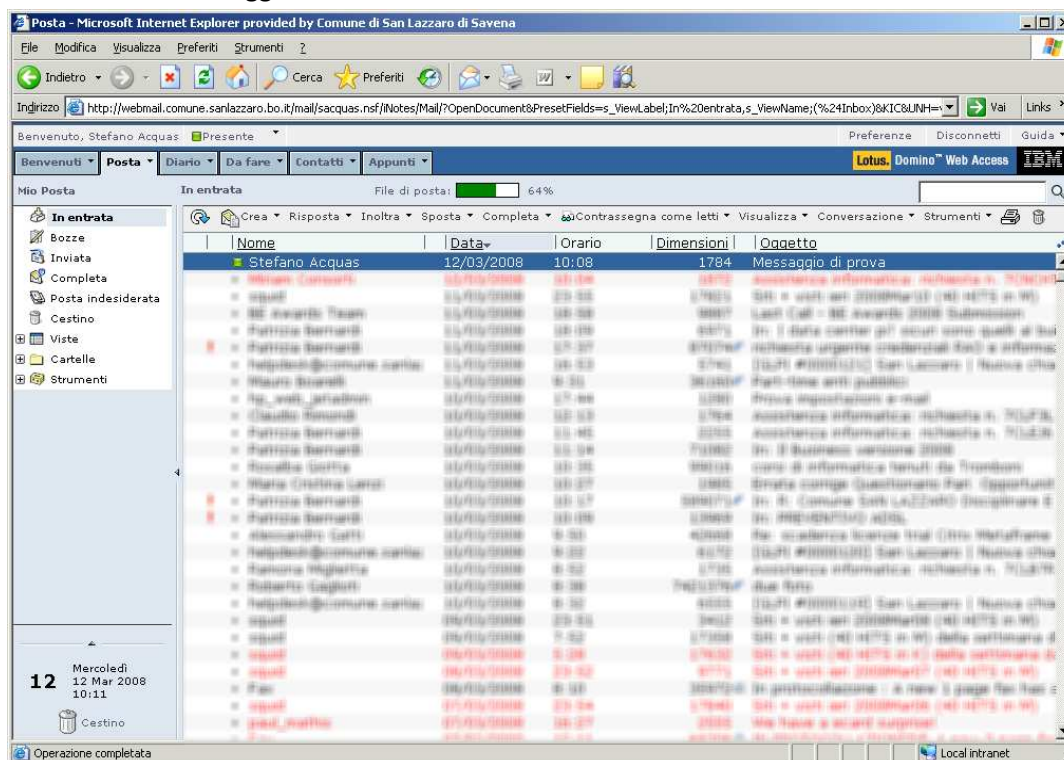
The screenshot shows a Windows-style dialog box titled "Assenza ufficio". It has a tabbed interface with two tabs: "Messaggio speciale" and "Eccezioni", with "Eccezioni" currently selected. The status "Stato corrente: Disabilitato" is displayed at the top. Below this, a text block explains that Notes can respond automatically to incoming mail when the user is not in the office and provides instructions on how to use the "Assenza dall'ufficio" agent. The "Eccezioni" section contains three options, each with a text input field and a dropdown arrow: 1) "Non rispondere automaticamente alla posta dagli indirizzi Internet:" with an unchecked checkbox. 2) "Non rispondere automaticamente alla posta da queste persone o gruppi:" with an empty text field. 3) "Non rispondere automaticamente alla posta indirizzata a questi gruppi:" with an empty text field. Below these is a section for "Non rispondere automaticamente se l'oggetto contiene queste frasi:" with an empty text field and instructions to position phrases on new lines and to check spelling. At the bottom are three buttons: "OK", "Annulla", and "Abilita".

7. Cliccare sul pulsante **Abilita**.
8. Cliccare sul pulsante **Ok**.

20 ALLEGATO L - ISTRUZIONI OPERATIVE SULLA CANCELLAZIONE DI UNA E-MAIL INDESIDERATA DAL DATABASE DI POSTA

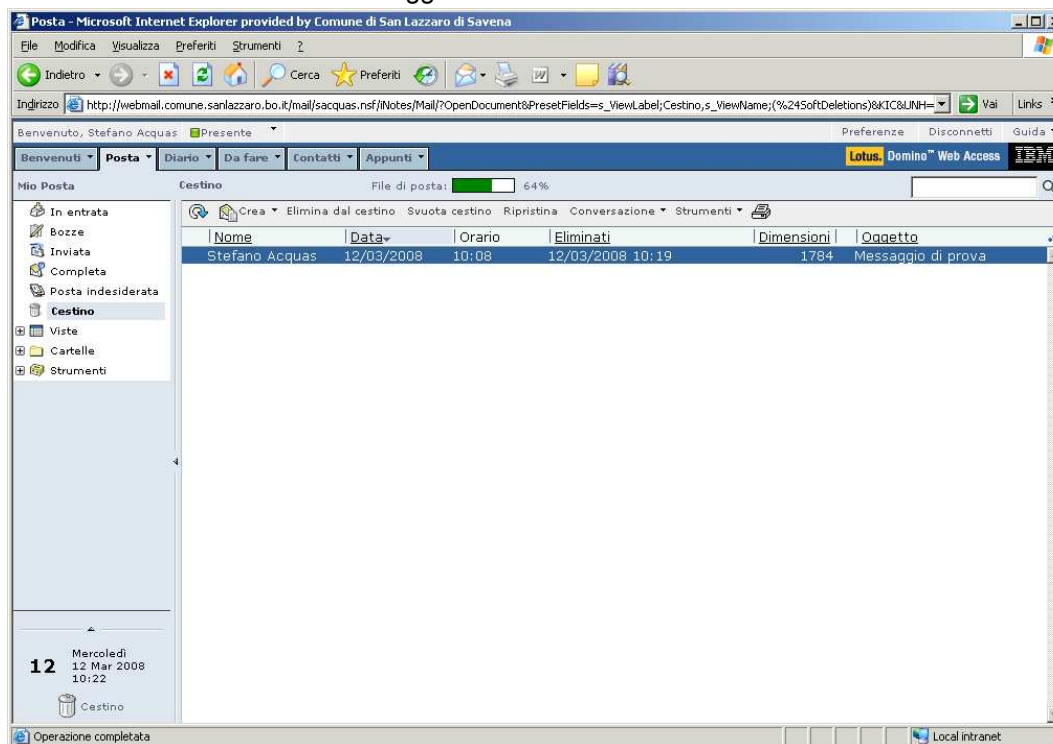
20.1 Lotus iNotes

1. Selezionare il messaggio da cancellare:



2. Cliccare sul pulsante di cancellazione: 
3. Cliccare sul pulsante **Cestino**:  **Cestino**
4. Verrà visualizzato il contenuto del **Cestino**

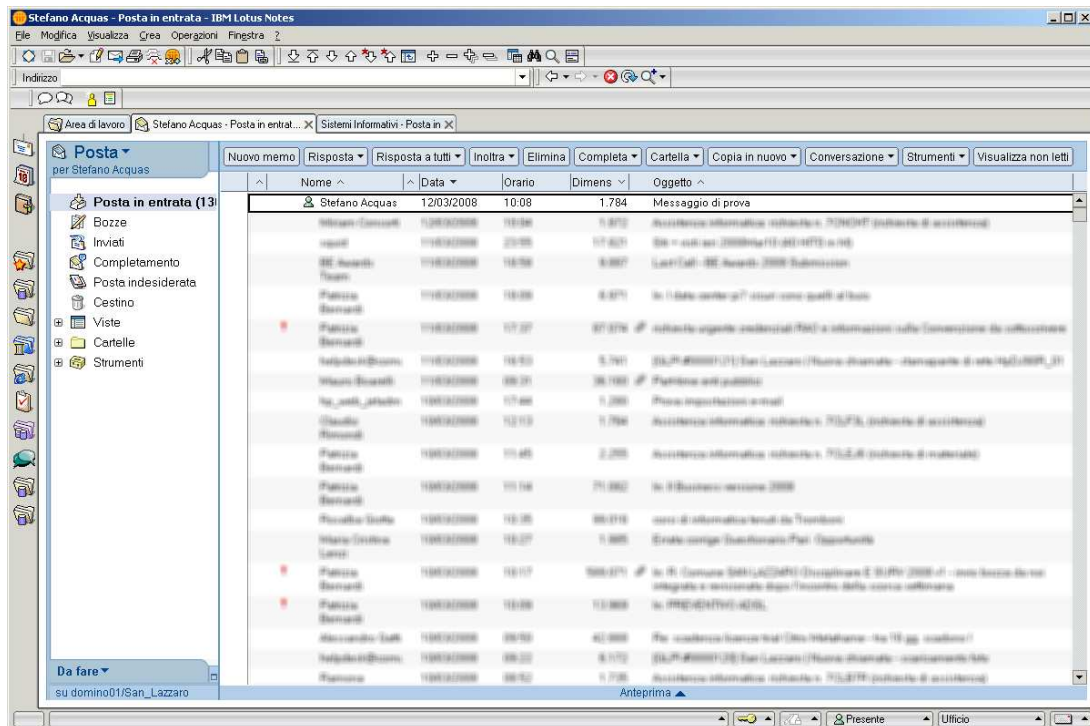
5. Selezionare nuovamente il messaggio cancellato:



6. Cliccare sul pulsante ***Elimina dal cestino***.

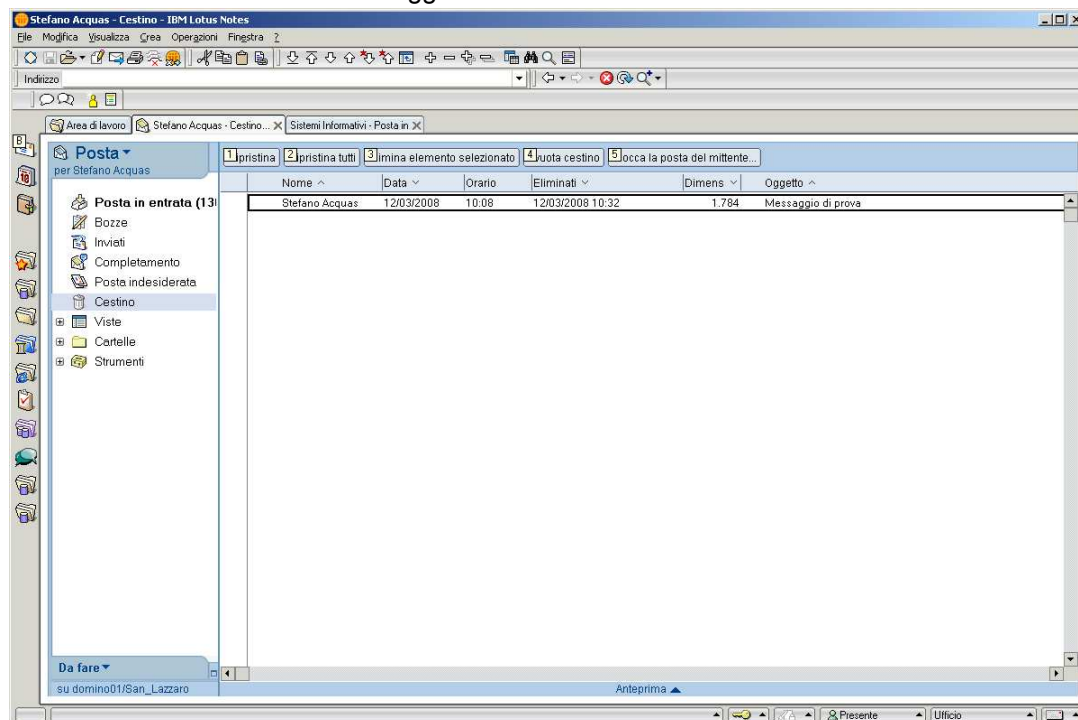
20.2 Lotus Notes

1. Selezionare il messaggio da cancellare:



2. Cliccare sul pulsante **Elimina**: 
3. Cliccare sul pulsante **Cestino**:  Cestino
4. Verrà visualizzato il contenuto del **Cestino**.

5. Selezionare nuovamente il messaggio cancellato:



6. Cliccare sul pulsante **Elimina elemento selezionato**:

Elimina elemento selezionato

21 ALLEGATO M - UNITÀ DI RETE

21.1 Unità di rete per il salvataggio di file e dati - esclusi i dati sensibili o giudiziari

U:	UNITÀ PER LE CARTELLE UTENTE da utilizzare per salvare dati utili al solo utente
F: (GRUPPI)	UNITÀ PER LE CARTELLE DI SETTORE da utilizzare per salvare dati utili al settore/servizio di appartenenza

21.2 Altre unità di rete - da non utilizzare per salvare dati

M: (CEDAF)	UNITA' PER I DATI UTILI AL FUNZIONAMENTO DEI PROGRAMMI DELLA DITTA CEDAF da non utilizzare per salvare dati
G: (GRADUS)	UNITA' PER I DATI UTILI AL FUNZIONAMENTO DEL PROGRAMMA GRADUS DELLA DITTA SOFTECH da non utilizzare per salvare dati
O: (SOSIA)	UNITA' PER I DATI UTILI AL FUNZIONAMENTO DEL PROGRAMMA SOSIA DELLA DITTA SOFTECH da non utilizzare per salvare dati
M: (CEDAF)	UNITA' PER I DATI UTILI AL FUNZIONAMENTO DEI PROGRAMMI DELLA DITTA CEDAF da non utilizzare per salvare dati
T:	UNITA' PER I DATI DEGLI UFFICI TECNICO ED URBANISTICA da non utilizzare per salvare dati
S: (SIT)	UNITA' PER I DATI DEGLI UFFICI TECNICO ED URBANISTICA da non utilizzare per salvare dati
S: (DATAGR)	UNITA' PER I DATI DEL VECCHIO PROGRAMMA DI CONTABILITA' (IN DISMISSIONE - attualmente disponibile solo per CED e Ragioneria) da non utilizzare per salvare dati
G: (GRADUS)	UNITA' PER I DATI UTILI AL FUNZIONAMENTO DEI PROGRAMMI DELLA DITTA SOFTECH da non utilizzare per salvare dati

V: (OTTICO)

**UNITA' PER I DATI UTILI AL FUNZIONAMENTO DEI PROGRAMMI
DELLA DITTA SIAV**

da non utilizzare per salvare dati

22 ALLEGATO N - AVVERTIMENTO AUTOMATICO PER LE E-MAIL

Il Comune di Castenaso avverte che la presente e-mail ha natura professionale. Ove necessario per esigenze lavorative, i messaggi inviati e ricevuti da questo account possono essere conosciuti da terze persone, diverse dall'intestatario dell'account, nell'ambito dell'organizzazione comunale.

Questo messaggio di posta elettronica contiene informazioni di carattere confidenziale rivolte esclusivamente al destinatario sopra indicato. E' vietato l'uso, la diffusione, distribuzione o riproduzione da parte di ogni altra persona.

Nel caso aveste ricevuto questo messaggio di posta elettronica per errore, siete pregati di segnalarlo immediatamente al mittente e distruggere quanto ricevuto (compresi i file allegati) senza farne copia.

Qualsivoglia utilizzo non autorizzato del contenuto di questo messaggio costituisce violazione dell'obbligo di non prendere cognizione della corrispondenza tra altri soggetti, salvo più grave illecito, ed espone il responsabile alle relative conseguenze.



COMUNE DI CASTENASO
Provincia di Bologna

Area Affari Generali

Segreteria Generale

CERTIFICATO DI PUBBLICAZIONE

**OGGETTO: DOCUMENTO PROGRAMMATICO SULLA SICUREZZA-DEC.LGS.196/2003-
AGGIORNAMENTO**

Copia della presente deliberazione N. 51/2010 del 25/03/2010 viene pubblicata all'Albo Pretorio per 15 gg. consecutivi dal 12/04/2010 al 27/04/2010, con numero di registro 187/2010 ai sensi e per gli effetti dell'art. 124 c. 1 D.Lgs 18.8.2000 n. 267.

La presente deliberazione è stata pubblicata nei termini sopra indicati. Contestualmente all'affissione è stata comunicata ai Gruppi consiliari ai sensi dell'art. 125 D.Lgs. 267/00

☒ Si attesta che la su estesa deliberazione è immediatamente esecutiva a partire dalla data 25/03/2010

Il Responsabile dell'Area Affari Generali
Dott.ssa Elisa Lui